A Theory of Physical Quantum Computation: The Quantum Computer Condition

Gerald Gilbert, Michael Hamrick and F. Javier Thayer
Quantum Information Science Group[*][†]
Mitre
260 Industrial Way West, Eatontown, NJ 07724 USA

Abstract. In this paper we present a new unified theoretical framework that describes the full dynamics of quantum computation. Our formulation allows any questions pertaining to the physical behavior of a quantum computer to be framed, and in principle, answered. We refer to the central organizing principle developed in this paper, on which our theoretical structure is based, as the *Quantum Computer Condition* (QCC), a rigorous mathematical statement that connects the irreversible dynamics of the quantum computing machine, with the reversible operations that comprise the quantum computation intended to be carried out by the quantum computing machine. Armed with the QCC, we derive a powerful result that we call the *Encoding No-Go Theorem*. This theorem gives a precise mathematical statement of the conditions under which fault-tolerant quantum computation becomes impossible in the presence of dissipation and/or decoherence. In connection with this theorem, we explicitly calculate a *universal* critical damping value for fault-tolerant quantum computation. In addition we show that the recently-discovered approach to quantum error correction known as "operator quantum error-correction" is a special case of our more general formulation. Our approach furnishes what we will refer to as "operator quantum fault-tolerance." In particular, we show how the QCC allows one to derive error thresholds for fault tolerance in a completely general context. We prove the existence of solutions to a class of time-dependent generalizations of the Lindblad equation. Using the QCC, we also show that the seemingly different circuit, graph- (including cluster-) state, and adiabatic paradigms for quantum computing are in fact all manifestations of a single, universal paradigm for all physical quantum computation.

[*] Research supported under MITRE Technology Program Grant 51MSR211.

[†] E-mail address: {ggilbert, mhamrick, jt}@mitre.org

Contents

1. Introduction

The promise inherent in quantum computing has stimulated a tremendous explosion of interest in the research community. Voluminous research has been carried out directed to many different problems associated with the development and properties of quantum computational algorithms. Parallel to these efforts, substantial investigations have been devoted to the problems associated with the development of actual quantum computing machines. A rigorous and fully general theory that connects quantum computing algorithms and quantum computing machines would be of considerable value.

In this paper we present a new unified theoretical framework that describes the full dynamics of quantum computation. Our formulation allows any questions pertaining to the physical behavior of a quantum computer to be framed, and in principle, answered. We refer to the central organizing principle developed in this paper, on which our theoretical structure is based, as the *Quantum Computer Condition* (QCC), a rigorous mathematical statement that connects the irreversible dynamics of the quantum computing machine, with the reversible operations that comprise the quantum computation intended to be carried out by the quantum computing machine.

The actual dynamics of the system that we intend to use as a practical quantum computing machine are those of an open quantum mechanical system, burdened with various dissipative and/or decoherence effects. The QCC provides a set of mathematical constraints that must be satisfied by a physical system if we intend to use that system as a quantum computing machine.

Armed with the QCC, we derive a powerful result that we call the *Encoding No-Go Theorem*. The Encoding No-Go theorem gives a precise mathematical statement of the conditions under which fault-tolerant quantum computation becomes impossible in the presence of dissipation and/or decoherence. We provide a rigorous definition of damping, which includes the phenomena of dissipation and decoherence, and explicitly calculate a *universal* critical damping value for fault-tolerant quantum computation. This fundamental theorem has deep formal significance. Moreover, it also furnishes criteria for solving diverse problems associated to actual physical quantum computer realizations, such as determining which practical design choices for quantum computing machines are not viable.

In addition we show that the recently-discovered approach to quantum error correction known as "operator quantum error-correction" (OQEC) is actually a special case of our general formulation. Our approach furnishes what we will refer to as "operator quantum fault-tolerance" (OQFT). In particular, we show how the QCC allows one to derive error thresholds for fault tolerance in a completely general context.

In this paper we define the concept of a *quantum component*, which allows us to study realistic implementations of quantum computers, in which decoherence and/or dissipative effects are present, using a dynamical equation of motion suitable for describing an open quantum system. By using the QCC, we are able to reconcile the apparent contradiction between: (1) the fact that quantum computations are specified by unitary transformations, the associated dynamics of which are intrinsically reversible, and (2) the fact that quantum computers, *qua* practical machines, are inevitably characterized by irreversible dynamics. The reconciliation suggests an analogy with the *fluctuation-dissipation theorem*, which relates irreversible dynamics to equilibrium properties in a large class of physical systems.

In this paper we present an existence proof for fundamental solutions to useful classes of *time-dependent* generalizations of the Lindblad equation. This provides a useful tool in analyzing a wide variety of open quantum mechanical systems.

Our framework is sufficiently general to encompass, and describe in a unified manner, the currently-known "paradigms" for quantum computation, including the *circuit-based ("two-way computing") paradigm*, the *graph state-based ("one-way computing") paradigm* and the *adiabatic quantum computer paradigm.* Using the QCC, we show by explicit construction that these seemingly different paradigms are in fact all manifestations of a single, universal paradigm for all physical quantum computation.[1]

2. The Quantum Computer Condition

2.1. Introduction. In this section we present the *Quantum Computer Condition*, a rigorous mathematical statement of the constraints that determine the viability of any practical quantum computing machine. To achieve the goal of practical quantum computation we must produce an actual physical device that implements a predetermined unitary operator U acting on some Hilbert space. The Quantum Computer Condition relates the unitary operator representing a quantum computation to the actual physical device intended to perform that computation.

The specification of U defines ideally the quantum computation to be performed by the quantum computing machine. Generically, the result of a quantum computation, U, is then used to carry out the probabilistic evaluation of some classical function. The complete quantum computation comprises a number of elements, including

- Preparation of a quantum state for initialization.
- Measurement of a quantum state for readout.

[1] In the particular case of the graph state-based paradigm (which includes cluster state-based models), we not only show that the paradigm is a manifestation of the unifying picture provided by the QCC, but also introduce a definition of graph state-based quantum computers that generalizes the graph state models previously defined in the literature.

- Various tasks that can be performed by classical computers, such as preprocessing of the data, or postprocessing of the output into some humanly comprehensible form.

However, the above list of elements are not what is "important" about quantum computers. Rather:

- The distinctive element of quantum computation is the "ability to perform quantum gates"(c.f. [**23**], §4.6).

Mathematically, a quantum gate is a unitary (hence reversible) operator U acting on a Hilbert space. The formally defined "gates," as such, are not "devices." They are concepts: they don't implement themselves. A machine is required to physically implement the abstractly defined unitary transformation. The actual, physical computing device intended to implement the transformation is described mathematically by a completely positive trace-preserving map, P, that transforms the input state to the output state. We will refer to a physically realizable device intended to implement an ideal quantum computation as a *quantum component.* In this paper we study realistic quantum components, in which decoherence and/or dissipative effects are present, using a dynamical equation of motion suitable for describing an open quantum system.[2] We must reconcile the fact, and apparent paradox, that a non-reversible mapping, P, is used to "implement" a reversible one, U.

2.2. The Motivation of the Quantum Computer Condition. Mathematically, a quantum computation is a unitary operator U in the unitary group of a Hilbert space. A quantum component is described by a completely positive trace-preserving map P which maps the set of trace class operators on the Hilbert space to itself. The map P accounts for decoherence and dissipation, as well as unitary evolution. We will subsequently discuss in more detail the actual form for P. In our analysis we will consider the action of P on density matrices $\rho \mapsto P \cdot \rho$ rather than on state vectors (and correspondingly the action of U on density matrices $\rho \mapsto U \rho U^\dagger$, rather than the action of U on state vectors). This is because, due to the presence of decoherence and/or dissipation, our system will almost always evolve into a mixed state, which can only be described by a density matrix ρ.[3]

In order to motivate the Quantum Computer Condition (QCC), let us first consider the abstractly-defined quantum computation itself, prescribed by the unitary

[2] In order to analyze the effects of dissipation and/or decoherence one must use *some* method of approximating the dynamics of the degrees-of-freedom comprising the rest of the universe "outside of" the quantum computer. This is of course because the complete, detailed, exact analytical solution to the Schrödinger equation of the universe, for all degrees-of-freedom, is not known. One reasonable approach is to construct a Lindblad-type equation, based on a presumption of underlying Markovian dynamics, in which environment degrees-of-freedom are traced over in such a way as to result in a first-order (in time) differential equation. In this paper, for definiteness, we utilize a generalized Lindblad-type equation to describe the environment: this is used merely in order to exemplify how one may take into account the effects of dissipation and/or decoherence. However, most of the results in our paper, including the crucial Encoding No-Go Theorem, are independent of this choice, and in particular are independent of the assumption of underlying Markovian dynamics.

[3] Other reasons for utilizing density matrices rather than state vectors include the generic importance in quantum information theory of trace-preserving completely positive maps (which restrict to transformations on density matrices), and the useful algebraic and analytic properties of density matrices (density matrices for instance form a weak-$*$ compact convex set).

operator U. This is assumed to be given, and is represented by

$$\text{abstract computation:}\;\; U\rho U^{\dagger}\;. \tag{1}$$

The action of the quantum component intended to effect the computation is represented by

$$\text{practical implementation:}\;\; P\cdot\rho\;. \tag{2}$$

Motivated by the notion of *having the machine implement the computation*, if we were to require that the identity

$$P\cdot\rho = U\rho U^{\dagger} \tag{3}$$

hold for all density states ρ, then the action of P would in fact be *identical* to the action of the unitary operator. This would imply that P preserves von Neumann entropy ([**32**], §5.3), and hence actually models a system with neither decoherence nor dissipation, which is not the case for a practical quantum computing machine. Thus, equation (3) cannot furnish the correct constraints for realistic quantum computation. We will accordingly refer to equation (3) as the *ersatz* quantum computer condition ($\mathcal{E}$QCC).[4]

More realistically, taking into account the inevitable presence of decoherence, we can require that (3) hold for some restricted set of density states. In this case, the solution set will correspond to decoherence-free subspaces. In order to analyze this, we must carefully distinguish between the two different Hilbert spaces that arise in this problem. The abstract quantum computation is defined on the Hilbert space of *logical* quantum states, H_{logical}, so that we have

$$U : H_{\text{logical}} \to H_{\text{logical}}. \tag{4}$$

In contrast, the presence of decoherence (which affects the actual device) necessitates that the completely positive trace-preserving map P (which represents the actual device) is associated to a different Hilbert space, H_{comp}, the states of which are referred to as *computational* quantum states. The decoherence-free subspace is contained within H_{comp}. (The specific decoherence is accounted for in the explicit form of P). As noted above, a consequence of the decoherence is that P operates on density matrices rather than on state vectors. Letting $\mathbf{T}(H_{\text{comp}})$ be the Banach space of trace-class operators on H_{comp}, we have

$$P : \mathbf{T}(H_{\text{comp}}) \to \mathbf{T}(H_{\text{comp}}). \tag{5}$$

In order to replace $\mathcal{E}$QCC (equation (3)) with an equation that properly incorporates decoherence effects so that it can be used to determine decoherence-free subspaces, we must introduce suitable encoding and decoding maps that connect the relevant Hilbert spaces. We can hope to find an encoding operator $\mathcal{M}_{\text{enc}}$ defined on a space of logical inputs and a decoding operator $\mathcal{M}_{\text{dec}}$ with values in a space of logical outputs, the actions of which are given by (here $\mathbf{T}(H_{\text{logical}})$ is the Banach space of trace-class operators on H_{logical}, analogous to $\mathbf{T}(H_{\text{comp}})$)

$$\mathcal{M}_{\text{enc}} : \mathbf{T}(H_{\text{logical}}) \to \mathbf{T}(H_{\text{comp}}) \tag{6}$$

[4] Although the $\mathcal{E}$QCC does not describe practical quantum computing machines, we note that it can be shown that in the finite-dimensional case, the set of ρ which satisfy (3) is an algebra $\mathfrak{A}_{P,U}$ which depends on both P and U. The details of how one explicitly obtains the algebra $\mathfrak{A}_{P,U}$ of solutions to (3) are given in Appendix C.

and

$$\mathcal{M}_{\text{dec}} : \mathbf{T}(H_{\text{comp}}) \to \mathbf{T}(H_{\text{logical}}), \tag{7}$$

such that (*cf* equation (3))

$$\mathcal{M}_{\text{dec}}(P \cdot (\mathcal{M}_{\text{enc}}(\rho))) = U \rho U^\dagger \tag{8}$$

for all logical inputs ρ. We will refer to equation (8) as the "encoded *ersatz* quantum computer condition (e$\mathcal{E}$QCC).[5] The existence of the encoding and decoding maps $\mathcal{M}_{\text{enc}}$ and $\mathcal{M}_{\text{dec}}$ is a consequence of the presumed existence of an associated decoherence-free subspace of H_{comp}, of dimension greater than or equal to the dimension of H_{logical}.

The meaning of e$\mathcal{E}$QCC given in eq.(8) is as follows. Given a chosen quantum computation, U, we wish to construct a physical "machine," P, that implements U. In order to do this we must find encoding and decoding maps $\mathcal{M}_{\text{enc}}$ and $\mathcal{M}_{\text{dec}}$ such that the equation is satisfied for all ρ. This is a crucial difference between eqs.(8) and (3): requiring that eq.(3) holds for all ρ implies a machine that preserves von Neumann entropy, does not dissipate heat and does not decohere, and thus does not describe a practical quantum computing device. In contrast, eq.(8) holds for all states ρ, but does so by making use of the encoding and decoding operators to map to a decoherence-free subspace. The e$\mathcal{E}$QCC (eq.(8)) formally holds for all density states ρ, similar to eq.(3), but the use of the encoding and decoding maps in eq.(8) effectively confines the solution to a restricted set in H_{comp}.

However, eq.(8) does not in general provide an acceptable condition to connect the dynamics of a practical quantum computing device to the constraints implied by the unitary operator U that defines the abstract quantum computation. *This is because the formulation presented by* (8) *does not address situations in which residual errors cannot be completely eliminated*, even with the use of decoherence-free subspaces, and/or other error correction methods [**20**], [**28**].

To recapitulate, eq.(3) describes a quantum computer that performs the required computation U, but only if the implementing device, described by the completely positive map P, neither dissipates heat nor decoheres. We thus reject this expression as a viable quantum computer condition because it describes a system that is effectively impossible to achieve. In contrast, eq.(8) describes a quantum computer that performs the required computation U, but only if the device described by the completely positive map P implements the required decoherence-free subspace with absolutely no residual errors. This does not provide a sufficiently general formulation: *we need to consider situations in which residual errors cannot be completely eliminated*.

2.3. The Presentation of the Quantum Computer Condition.

We wish to allow for the likelihood that, even if a decoherence-free subspace can be found, and even if error correction procedures are applied, there will still be residual errors characterizing the operation of the quantum computer. Such a situation may arise even if error correction is correctly applied: for instance, in the application of concatenated error codes, one iterates the concatenation process until the error probability is reduced to a value that is deemed "acceptable" [**28**], [**24**]. This final error probability, though small, is not exactly zero. The important point is that

[5] Note that no encoding map is required on the right-hand side of equation (8) since the unitary U by definition acts on H_{logical}.

it is prudent to write down our quantum computer condition so as to reflect the inevitable survival of some amount of residual error.

In order to quantify the degree to which the actual computational device, represented by P, *cannot exactly* (because of residual error) implement the ideal quantum computation, represented by U, we consider the following difference (*cf* eq.(8))

$$\mathcal{M}_{\text{dec}}(P \cdot (\mathcal{M}_{\text{enc}}(\rho))) - U\rho U^{\dagger}. \tag{9}$$

We now compute for this difference a suitable norm on matrices (this norm is made more precise below), as

$$\|\mathcal{M}_{\text{dec}}(P \cdot (\mathcal{M}_{\text{enc}}(\rho))) - U\rho U^{\dagger}\|. \tag{10}$$

This quantity is of fundamental importance: *it is a measure of the inaccuracy of the implementation of U by P.* It tells us how well a practical quantum computing device actually implements an ideally-defined quantum computation. We will refer to the scalar quantity given by (10) as the *implementation inaccuracy* associated to the pair U and P. In connection with this, we introduce a parameter, α, to specify the maximum tolerable implementation inaccuracy, so that we have

$$\|\mathcal{M}_{\text{dec}}(P \cdot (\mathcal{M}_{\text{enc}}(\rho))) - U\rho U^{\dagger}\| \leq \alpha. \tag{11}$$

2.3.1. *Formal Statement of the Quantum Computer Condition (QCC).* Motivated by the above considerations, we now introduce and formally define an inequality of fundamental importance in the theory of quantum computation that we will refer to as the *Quantum Computer Condition.* We will formally designate this condition by $\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$. In the following, we will impose no constraint on the dimensionality of the Hilbert space, and in particular we allow Hilbert spaces of infinite dimensions. Let U be a unitary on H_{logical} and P be a trace-preserving completely positive map on $\mathbf{T}(H_{\text{comp}})$. Let $\mathcal{M}_{\text{enc}} : \mathbf{T}(H_{\text{logical}}) \to \mathbf{T}(H_{\text{comp}})$ and $\mathcal{M}_{\text{dec}} : \mathbf{T}(H_{\text{comp}}) \to \mathbf{T}(H_{\text{logical}})$ be completely-positive, trace-preserving encoding and decoding maps (with no further restrictions of any kind on the encoding and decoding maps). The Quantum Computer Condition, $\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$, holds iff for all density matrices $\rho \in \mathbf{T}(H_{\text{logical}})$, we have

$$\|\mathcal{M}_{\text{dec}}(P \cdot (\mathcal{M}_{\text{enc}}(\rho))) - U\rho U^{\dagger}\|_1 \leq \alpha, \tag{12}$$

where $\mathbf{T}(H_{\text{comp}})$ and $\mathbf{T}(H_{\text{logical}})$ are the Banach spaces of trace-class operators on H_{comp} and H_{logical}, respectively, and $\| \cdot \|_1$ is the Schatten 1-norm defined in Appendix A.

It should be noted that an alternate measure of distance between density matrices to that provided by the Schatten 1-norm is given by the fidelity function [**23**]. One could write an alternate form of the QCC in terms of the fidelity that would be essentially equivalent to the form of the QCC given in (12) above. Using an obvious notation to denote the QCC written with each of these definitions of distance, the two forms are related as follows. Given a quartet $\{P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}\}$, one can show that if $\mathbf{QCC}_{\text{Schatten}}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$ is satisfied, then the fidelity-based version of QCC given by $\mathbf{QCC}_{\text{fidelity}}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha')$ is also satisfied, where $\alpha' = \alpha'(\alpha)$ is a function of α. The form of QCC based on the Schatten 1-norm given above in (12) is more convenient for our purposes for a number of mathematical reasons, including the fact that that the fidelity, as such, is not a proper norm. For instance, the statement and proof of the Encoding No-Go Theorem carried out in

§3 below are more conveniently presented making use of the form of the QCC based on the Schatten norm.

Note that $\mathcal{M}_{\mathrm{enc}}$ and $\mathcal{M}_{\mathrm{dec}}$ do not represent *physical* operations: all physical operations are carried out by the quantum component P. If the proper distinction between these maps and P is not observed, one could include the *entire* computation in the definition of the maps, with the absurd conclusion that any quantum computation could be performed in the absence of any real hardware.

2.3.2. *Some implications of the QCC.* The QCC is a remarkably powerful expression. It constitutes a kind of "master expression" for physical quantum computation. The inequality (12) concisely incorporates a complete specification of the full dissipative, decohering dynamics of the actual, practical device used as the quantum computing machine, a specification of the ideally-defined quantum computation intended to be performed by the machine, and a quantitative criterion for the accuracy with which the computation must be executed given the inevitability of residual errors surviving even after error correction has been applied.

Making use of the QCC, one can state and prove (we do this is in §3, the next section of the paper) a fundamental and powerful theorem in the subject of quantum computing, the *Encoding No-Go Theorem*. This no-go theorem gives a precise mathematical statement of the conditions under which fault-tolerant quantum computation becomes impossible in the presence of dissipation and/or decoherence. Apart from its formal significance, the theorem can be used to compare different proposed physical approaches to actually building a quantum computing machine, with the no-go condition furnishing a criterion for the practical engineering viability of various choices.

As a further indication of the power and general applicability of the QCC, we show that one can apply it to the known, seemingly distinct "paradigms" for quantum computing, based on (1) the use of quantum circuits built up out of quantum gates (the *circuit-based paradigm*, or "two-way" quantum computing), (2) the use of graph states or cluster states (the *graph state-based paradigm*, or "one-way" quantum computing) and (3) the use of specially chosen Hamiltonians describing adiabatic dynamics (the *adiabatic quantum computer paradigm*). The QCC allows one to show that these apparently different definitions of a quantum computer are in fact manifestations of the same underlying formulation: *there is only one paradigm for quantum computers*. The application of the QCC to different quantum computing paradigms is discussed in §5.

The encoding-decoding pair $\mathcal{M}_{\mathrm{enc}}$ and $\mathcal{M}_{\mathrm{dec}}$ that appear in the QCC are defined quite generally as completely positive trace-preserving maps. This formulation is sufficiently general to encompass all possible encodings associated with standard quantum error correction (QECC) techniques, decoherence-free subspaces and noiseless subsystems. More generally still, we show below in §2.3.3 that the recently discovered approach known as "operator quantum error correction" (OQEC) is in fact a special case of our more general QCC formulation. In addition the QCC can be used to extend OQEC to what we will refer to as "operator quantum fault-tolerance" (OQFT). In particular, we show in §6 below how the QCC allows one to derive error thresholds for fault tolerance in a completely general context.

Another significant consequence of the QCC is that it resolves the apparent paradox that the quantum computations we wish to perform are defined by reversible operators, but the actual devices that we must use to execute the computations are necessarily described by irreversible maps. We note that this is reminiscent of the *fluctuation-dissipation theorem*, which relates irreversible dynamics to equilibrium properties in a large class of physical systems. Inspection of (12) reveals that the paradox is resolved through the transformations provided by the encoding and decoding maps associated to the QCC. Roughly speaking, reversible behavior of the actual device is enabled only on the code subspace defined by $\mathcal{M}_{\text{enc}}$ and $\mathcal{M}_{\text{dec}}$.

Note that if one describes quantum computing solely in terms of the unitary transformations that define the computations, it is not too surprising that the resulting computational model is in some way "powerful." After all, unitary transformations on finite dimensional spaces include such powerful operations as the discrete Fourier transform which are known to play an important role in number theoretic problems. Rather than regarding the power of the ideally-defined quantum computation as the remarkable thing, the *truly* remarkable thing would be the construction of an inherently irreversible device that actually implements the reversible, unitary map to a specified level of accuracy. It is this possibility that our QCC expresses and makes mathematically precise. The QCC can thus be used to formulate and prove assertions about the physical solvability of particular computational problems.

2.3.3. *Operator quantum error correction (OQEC) as a special case of QCC.* The recently developed theory of operator quantum error correction [**18**], [**19**] unifies many apparently disparate approaches to the practical problem of dealing with errors in quantum information. Among these approaches are quantum error correction, decoherence free subspaces and noiseless subsystems. Here we show that OQEC is in fact a special case of the general statement of the QCC. In this section we demonstrate that the entire formalism of OQEC can be obtained from QCC by choosing $\mathcal{M}_{\text{enc}}$ and $\mathcal{M}_{\text{dec}}$ as described below, and by setting setting $U = I$ and $\alpha = 0$ in the QCC, so that the reduction QCC → OQEC is given by:

$$\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha) \to \mathbf{QCC}(P, I, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, 0)\ . \tag{13}$$

In the scheme of OQEC, the techniques of (standard) quantum error correction, decoherence free subspaces and noiseless subsystems are subsumed under the unified concept of "correctability." This is defined formally as follows. Let H_{comp} be a Hilbert space with a decomposition $H_{\text{comp}} = \left(H^A \otimes H^B\right) \oplus K$, where H^A, H^B and K are discussed in the following paragraph. We identify this as the computational space H_{comp} of this paper because, as we shall see below, it describes the space on which the real physical processes of error and recovery operate. Let $\mathfrak{S}$ be the semigroup given by

$$\mathfrak{S} = \{\sigma \in \mathbf{L}(H_{\text{comp}}) : \exists \sigma^A \in \mathbf{L}(H^A), \exists \sigma^B \in \mathbf{L}(H^B),\ \text{such that } \sigma = \sigma^A \otimes \sigma^B\}\ , \tag{14}$$

where $\mathbf{L}(\cdot)$ is the space of bounded operators[6] on the appropriate Hilbert space, with the operator norm, and let $\mathcal{E}$ and $\mathcal{R}$ be completely-positive, trace preserving maps

[6] In §2.3.3 of this paper we assume (following [**19**]) that all Hilbert spaces are finite-dimensional. Although not discussed in [**19**], it is important to note that if one makes this

on $\mathbf{L}(H_{\mathrm{comp}})$ corresponding to error processes and recovery processes, respectively. We say that $\mathfrak{S}$ is correctable for $\mathcal{E}$ iff

$$\forall \sigma \in \mathfrak{S},\ (\mathrm{Tr}_A \circ \mathcal{P}_{\mathfrak{S}} \circ \mathcal{R} \circ \mathcal{E})\, \sigma = \mathrm{Tr}_A \sigma\ , \tag{15}$$

where $\mathcal{P}_{\mathfrak{S}}$ effectively projects density matrices onto the $H^A \otimes H^B$ subspace of H_{comp}.

Physically speaking, H^B is the Hilbert space which carries the information to be protected from errors, the "noiseless subsystem," while H^A is the Hilbert space on which the errors are permitted to operate freely, the "noisy subsystem." K is the orthogonal complement of $H^A \otimes H^B$ in H_{comp} and is simply projected out by $\mathcal{P}_{\mathfrak{S}}$. Thus, in (15), $\mathrm{Tr}_A\sigma$ represents the quantum information which is to be protected. The left side of (15) describes the effect of allowing errors to operate on the full state σ, and then applying recovery procedures. (The projection and the trace simply extract the state of the noiseless subsystem.) According to (15), correctability thus means that the recovery procedure does in fact recover the state of the noiseless subsystem, $\mathrm{Tr}_A\sigma$, without error.

As we now show, the definition of correctability is actually a special case of the QCC. Note first that correctability, as defined above, applies to a quantum channel as opposed to a quantum computer. It describes the transportation of a quantum state in a noisy environment as opposed to the "processing" of a quantum state so as to implement a quantum computation. In order to make the connection with the QCC, we may therefore think of the quantum channel as a quantum computer that implements the identity operation:

$$U = I_{H_{\mathrm{logical}}} \tag{16}$$

In the definition of correctability, the part of the state containing the information of interest is recovered without error. This corresponds to taking $\alpha = 0$ in the QCC. Note that, as discussed above, this is not practically achievable for quantum computers. This is less obviously an issue for the theory of operator error correction as currently formulated [**18**], [**19**], since that theory addresses a relatively circumscribed set of circumstances in which one is concerned with transporting quantum states rather than implementing a quantum computation. In particular, the error process $\mathcal{E}$, which is specified in advance, only operates *once* on the quantum state being transported. Error processes associated with the constituent parts of quantum computers operate each time the constituent part operates on the the quantum state being processed. The problem of fault tolerant quantum computation is inherently more complex than the problem of error correction/protection for a quantum channel. We will discuss this more fully in §6 below.

Setting $U = I$ and $\alpha = 0$ in the quantum computer condition, we obtain

$$\|\,(\mathcal{M}_{\mathrm{dec}} \circ P \circ \mathcal{M}_{\mathrm{enc}})\, \rho - \rho\|_1 = 0, \tag{17}$$

or

$$(\mathcal{M}_{\mathrm{dec}} \circ P \circ \mathcal{M}_{\mathrm{enc}})\, \rho = \rho\ , \tag{18}$$

where $\rho \in L(H_{\mathrm{logical}})$.[7]

assumption, there is then no need to distinguish between bounded operators in $L(\cdot)$ and trace-class operators in $T(\cdot)$. This distinction is important in the other sections of our paper where we allow Hilbert spaces of infinite as well as finite dimensionality.

[7] As noted in the previous footnote, we are assuming in §2.3.3 that H_{logical} is finite-dimensional.

We now proceed to define the encoding map $\mathcal{M}_{\text{enc}}$. For this purpose we define a map $W_{\text{enc}} : \mathbf{L}(H_{\text{logical}}) \to \mathbf{L}(H^B)$ that encodes the logical quantum state ρ in a state σ^B of the noiseless subsytem. We further define a map $W_{\text{adj}}(\sigma^A) : \mathbf{L}(H^B) \to \mathbf{L}(H^A \otimes H^B)$ that adjoins an arbitrary state σ^A of the noisy subsystem to the state σ^B, that is

$$W_{\text{adj}}(\sigma^A) : \sigma^B \mapsto \sigma \equiv \sigma^A \otimes \sigma^B \tag{19}$$

We then define the full encoding map that appears in the QCC as follows:

$$\mathcal{M}_{\text{enc}} \equiv W_{\text{adj}}(\sigma^A) \circ W_{\text{enc}} \tag{20}$$

The map P characterizes the dynamics of the physical computer, which in this case is just the (noisy) channel followed by the recovery procedure:

$$P \equiv \mathcal{R} \circ \mathcal{E} \tag{21}$$

We note that the current formulation of the theory of operator quantum error correction implicitly assumes that the recovery process $\mathcal{R}$ can be implemented without error, even though this requires, in general, that coherent operations be performed on entangled quantum states. Once again, the emphasis on error correction alone avoids the more difficult issue of achieving true fault tolerance.

Finally we define the decoding map as:

$$\mathcal{M}_{\text{dec}} = W_{\text{enc}}^{-1} \circ \text{Tr}_A \circ \mathcal{P}_{\mathfrak{S}} \ , \tag{22}$$

which extracts the state of the noiseless subsystem and decodes it to obtain a state in the logical space $\mathbf{L}(H_{\text{logical}})$.

With the above definitions, the QCC becomes

$$\left(W_{\text{enc}}^{-1} \circ \text{Tr}_A \circ \mathcal{P}_{\mathfrak{S}} \circ \mathcal{R} \circ \mathcal{E} \circ W_{\text{adj}}(\sigma^A) \circ W_{\text{enc}}\right) \rho = \rho \ . \tag{23}$$

Applying W_{enc} to both sides, and recalling that $W_{\text{enc}}\rho = \sigma^B = \text{Tr}_A\sigma$, we obtain

$$\left(\text{Tr}_A \circ \mathcal{P}_{\mathfrak{S}} \circ \mathcal{R} \circ \mathcal{E} \circ W_{\text{adj}}(\sigma^A) \circ W_{\text{enc}}\right) \rho = \text{Tr}_A\sigma \ . \tag{24}$$

Noting that $W_{\text{adj}}(\sigma^A) \circ W_{\text{enc}}\rho = \sigma$, we obtain the correctability condition of [**18**], [**19**]:

$$\left(\text{Tr}_A \circ \mathcal{P}_{\mathfrak{S}} \circ \mathcal{R} \circ \mathcal{E}\right) \sigma = \text{Tr}_A\sigma \ . \tag{25}$$

In summary, we have shown that the formalism of operator quantum error correction actually arises as a special case of an underlying definition of physical quantum computation given by the QCC. In addition, examination of operator quantum error correction (OQEC) from the perspective of the QCC reveals limitations and restrictions implicit to the formalism of operator quantum error correction, and inherited from the previously known, standard approaches to error correction (QECC). These limitations render direct application of either OQEC or QECC to questions of fault tolerance somewhat problematic, whereas the QCC approach is more immediately applicable. Thus, the QCC enables one to generalize OQEC to operator fault tolerance (OQFT).

3. The Encoding No-Go Theorem

3.1. Introduction. Armed with the QCC, in this section we state and prove a theorem of crucial importance in the theory of physical quantum computation. This is the *Encoding No-Go Theorem*, which gives a precise mathematical statement of the conditions under which fault-tolerant quantum computation becomes impossible in the presence of damping. Damping, for which we provide a mathematically rigorous definition below, includes the effects of dissipation and decoherence. The No-Go theorem for a completely positive trace-preserving map P corresponding to a putative quantum computing device then asserts that, in the presence of sufficient damping, the quantum computer condition $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$ (*cf* (12)) cannot be satisfied for any encoding-decoding pair, unless H_{logical} has dimension 1: there is then effectively no quantum computer. (In the case that $\dim H_{\mathrm{logical}} = 1$ we are of course unable to define a meaningful quantum computation at all.) As part of the No-Go Theorem we explicitly calculate a *universal* critical damping value for fault-tolerant quantum computation. We precisely state and prove this theorem in the remainder of §3.

3.2. Encoding and Decoding Maps. An encoding-decoding pair are completely positive, trace-preserving maps

$$\begin{aligned} \mathcal{M}_{\mathrm{enc}} &: \mathbf{T}(H_{\mathrm{logical}}) \to \mathbf{T}(H_{\mathrm{comp}}) \\ \mathcal{M}_{\mathrm{dec}} &: \mathbf{T}(H_{\mathrm{comp}}) \to \mathbf{T}(H_{\mathrm{logical}}). \end{aligned} \tag{26}$$

Encoding-decoding pairs provide the link between a completely positive map $P : \mathbf{T}(H_{\mathrm{comp}}) \to \mathbf{T}(H_{\mathrm{comp}})$ corresponding to a physical device and a unitary operator $U : H_{\mathrm{logical}} \to H_{\mathrm{logical}}$ corresponding to a quantum computation. We will place no further restrictions on encoding-decoding pairs. Now, suppose $\mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}$ is an encoding-decoding pair. Then the adjoint maps $\mathcal{M}_{\mathrm{dec}}^{\mathrm{t}}$, $\mathcal{M}_{\mathrm{enc}}^{\mathrm{t}}$ are unit preserving completely positive maps. (Adjoint maps of completely positive maps are defined in (132) in Appendix B.)

3.3. Damping and γ-damping. Dissipative and decohering effects are consequences of *damping*. To begin the development of the No-Go Theorem, we introduce a mathematically precise definition of the damping of a quantum mechanical system, to which we refer as γ-damping.

Definition 3.1. Let H be a Hilbert space. A completely positive trace-preserving map $P : \mathbf{T}(H) \to \mathbf{T}(H)$ is γ*-damped* iff there is an abelian von Neumann algebra $\mathfrak{A} \subseteq \mathbf{L}(H)$ such that for all $T \in \mathbf{L}(H)$, there is an $S_T \in \mathfrak{A}$ such that

$$\|P^{\mathrm{t}}(T) - S_T\|_\infty \leq \gamma \|T\|_\infty, \tag{27}$$

where the operator norm $\|\cdot\|_\infty$ is defined in Appendix A. Note that larger values of γ correspond to less damping of the system.

To make contact with the physically intuitive notion of damping, we apply this definition to the example of the simple harmonic oscillator subject to phase damping. For such an harmonic oscillator, the ijth element of the density matrix, $\rho_{ij} = \langle i|\rho|j\rangle$, decays exponentially as $e^{-\kappa(i-j)^2}$, where we are working in the basis of energy eigenstates identified by the labels i and j. The quantity κ is characteristic of the specific oscillator and its coupling to the environment. The completely positive map P transforms the initial, general density matrix for the system into a density matrix with exponentially-decaying off-diagonal elements. Under the influence of damping, as the off-diagonal states of the oscillator decay and approach zero, the density matrix converges to a diagonal density matrix in the $\{ij\}$ basis specified above. This is true for all initial configurations of the oscillator, and thus the damping process tends to an abelian set of final configurations. (The damping parameter κ that characterizes the decay of the off-diagonal elements of the density matrix is related to the quantity γ that appears in (27). As noted above, larger values of γ correspond to less damping and hence smaller values of κ.)

3.4. No-Go Theorem for Encodings. We now state the main result of §3: *the Encoding No-Go Theorem.*

Theorem 3.2 (**The Encoding No-Go Theorem**).
Suppose that $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$ *holds. If* $P : \mathbf{T}(H_{\mathrm{comp}}) \to \mathbf{T}(H_{\mathrm{comp}})$ *is* γ*-damped and* $2\gamma + \alpha < \sqrt{2}/4$*, then* H_{logical} *has dimension* 1*.*

To prove the Encoding No-Go Theorem, we first derive in §3.5 a number of general mathematical results on completely positive maps. We then apply these specifically to obtain a proof of the Encoding No-Go Theorem in §3.6 below.

3.5. Completely Positive Maps with Abelian Factorizations. We begin with the following lemma, which furnishes a superoperator version of the definition of γ-damping. For any abelian von Neumann algebra $\mathfrak{A} \subseteq \mathbf{L}(H)$ there is a unit-preserving completely positive projection operator $\mathbf{E}_{\mathfrak{A}} : \mathbf{L}(H) \to \mathfrak{A}$. This fact is elementary, but also follows from injectivity [**7**] of such algebras, in the case H is separable.

Lemma 3.3. *If* P *is* γ*-damped,* $\mathfrak{A}$ *is as given in Definition 3.1 and* $\mathbf{E}_{\mathfrak{A}} : \mathbf{L}(H) \to \mathfrak{A}$ *is a unit-preserving completely positive projection mapping* $\mathbf{E}_{\mathfrak{A}} : \mathbf{L}(H) \to \mathfrak{A}$*, then*

$$\|P^{\mathrm{t}}(T) - \mathbf{E}_{\mathfrak{A}} P^{\mathrm{t}}(T)\|_\infty \leq 2\gamma \|T\|_\infty. \tag{28}$$

Proof. Note that $\mathbf{E}_{\mathfrak{A}}$ is a linear mapping of norm ≤ 1 and thus

$$\begin{aligned} \|P^{\mathrm{t}}(T) - \mathbf{E}_{\mathfrak{A}} P^{\mathrm{t}}(T)\|_\infty &\leq \|P^{\mathrm{t}}(T) - S_T\|_\infty + \|S_T - \mathbf{E}_{\mathfrak{A}} P^{\mathrm{t}}(T)\|_\infty \\ &\leq \gamma \|T\|_\infty + \|\mathbf{E}_{\mathfrak{A}} S_T - \mathbf{E}_{\mathfrak{A}} P^{\mathrm{t}}(T)\|_\infty \\ &\leq 2\gamma \|T\|_\infty, \end{aligned} \tag{29}$$

as claimed. □

In the remainder of this section we prove an important technical result used in the proof of the no-go theorem, namely that completely positive maps $F : \mathbf{L}(H) \to \mathbf{L}(H)$, which factor through completely positive maps into abelian von Neumann algebras, cannot be used to approximate unitary operators U on H if $\dim(H) \geq 2$. More precisely, we will show that for any $\beta < \sqrt{2}/4$, there is at least one non-zero operator T for which

$$\|U^\dagger T U - F(T)\|_\infty \geq \beta \; \|T\|_\infty. \tag{30}$$

We first define what it means for a completely positive map to factor through an abelian von Neumann algebra:

Definition 3.4. Let A be a C*-algebra with a multiplicative unit. A unit preserving completely positive map $F : A \to A$ has an *abelian factorization* (or briefly is abelian factorizable) iff there is an abelian von Neumann algebra $\mathfrak{B}$ and unital completely positive maps $Q : A \to \mathfrak{B}$, $R : \mathfrak{B} \to A$ such that F is the composition $R \circ Q$.

If $F : \mathbf{L}(H) \to \mathbf{L}(H)$ is abelian factorizable, then it follows from the definition that for any unit-preserving completely positive maps Q, R, the completely positive map $Q \circ F \circ R$ is abelian factorizable. We begin by providing a characterization of abelian factorizable maps.

Proposition 3.5. *Let A be an arbitrary* C**-algebra with multiplicative unit. A unit preserving completely postive map $F : A \to A$ factors through a finite-dimensional abelian von-Neumann algebra iff there are unit preserving positive linear functionals $\rho_1, \dots, \rho_m \in A^\dagger$ and positive elements $G_1, \dots, G_m \in A$ of norm ≤ 1, such that $\sum_{i=1}^m G_i = I$ and*

$$F(T) = \sum_{i=1}^{m} \rho_i(T) G_i \quad \forall T \in A. \tag{31}$$

Proof. We first note that positive maps from an abelian C*-algebra or into an abelian C*-algebra are automatically completely positive (see [**29**],[**6**]). Thus the map F given by Equation (31) is completely positive. Let $\mathfrak{B}$, $Q : A \to \mathfrak{B}$, $R : \mathfrak{B} \to A$ as in Definition 3.4, but with $\mathfrak{B}$ finite dimensional and let $E_1, \dots, E_m$ be the minimal non-zero projections of $\mathfrak{B}$. Then

$$F(T) = R\Big(\sum_{i=1}^{m} E_i Q(T) E_i\Big) = R\Big(\sum_{i=1}^{m} \rho_i(T) E_i\Big) = \sum_{i=1}^{m} \rho_i(T) R(E_i). \tag{32}$$

Letting $G_i = R(E_i)$,

$$\sum_{i=1}^{m} G_i = \sum_{i=1}^{m} R(E_i) = R\Big(\sum_{i=1}^{m} E_i\Big) = I. \tag{33}$$

This completes the proof. □

In general, unit-preserving completely positive maps with arbitrary abelian factorizations can be approximated by maps of the form (31).

Proposition 3.6. *If a completely positive map $F : A \to A$ has an abelian factorization, then there is a generalized sequence of maps $\{F_\kappa\}_{\kappa \in K}$ each having the form $F_\kappa(T) = \sum_{i=1}^m \rho_i(T) G_i$ which converges to F in the point-norm topology, that is for each $T \in A$, $F_\kappa(T) \to F(T)$ in the norm of A.*

Proof. Let $\mathfrak{B}$, $Q : A \to \mathfrak{B}$, $R : \mathfrak{B} \to A$ as in Definition 3.4. Given $T_1, \dots, T_m \in A$, let $\mathfrak{B}_0$ be a finite dimensional abelian von-Neumann subalgebra of $\mathfrak{B}$ and $\mathbf{E}$ a linear projection operator[8] $\mathfrak{B} \to \mathfrak{B}_0$ such that

$$\|Q(T_i) - \mathbf{E}(Q(T_i))\|_\infty \leq \epsilon. \tag{34}$$

Since Q is contractive, it follows that

$$\|F(T_i) - R \circ \mathbf{E} \circ Q(T_i)\|_\infty \leq \epsilon. \tag{35}$$

Now apply the preceding result. □

[8] These operators are sometimes referred to as *conditional expectations*.

Assume H is a finite dimensional Hilbert space. We will consider trace functionals on two distinct spaces of operators: one on the space $\mathbf{L}(H)$, which we denote by tr, and the other on the space $\mathbf{L}(\mathbf{L}(H))$ of linear mappings $\mathbf{L}(H) \to \mathbf{L}(H)$, which we denote $\mathrm{tr}_{\mathrm{oper}}$. We will prove that abelian factorizable completely positive maps cannot approximate the identity map on $\mathbf{L}(H)$. To do this we will show that the trace functional $\mathrm{tr}_{\mathrm{oper}}$ separates, in a sense to be made precise in the next paragraph, the identity operator on $\mathbf{L}(H)$ from abelian factorizable completely positive F. Note that $\mathrm{tr}_{\mathrm{oper}}(I_{\mathbf{L}(H)}) = \dim^2(H)$.

Lemma 3.7. *Suppose the Hilbert space H has finite dimension n. For any unit-preserving abelian-factorizable completely positive map $F : \mathbf{L}(H) \to \mathbf{L}(H)$,*

$$\mathrm{tr}_{\mathrm{oper}}(F) \leq n. \tag{36}$$

Proof. It suffices to prove this for F which have the form (31). Referring to that representation, each positive functional ρ_i can be represented by a non-negative operator S_i as follows:

$$\rho_i(T) = \mathrm{tr}(T S_i), \tag{37}$$

Since $\rho_i(I) = 1$, S_i also has unit trace and in particular, $S_i \leq I$. Moreover $\sum_{i=1}^m G_i = I_H$. Now

$$\begin{aligned}
\mathrm{tr}_{\mathrm{oper}}(P) &= \sum_{i=1}^m \mathrm{tr}(S_i G_i) \\
&= \sum_{i=1}^m \mathrm{tr}(G_i^{1/2} S_i G_i^{1/2}) \\
&\leq \sum_{i=1}^m \mathrm{tr}(G_i^{1/2} G_i^{1/2}) \\
&= \sum_{i=1}^m \mathrm{tr}(G_i) = \mathrm{tr}(I_H) = n.
\end{aligned} \tag{38}$$

□

The previous lemma gives us a lower bound on the trace of $I - F$ for F abelian factorizable:

$$\mathrm{tr}_{\mathrm{oper}}(I - F) \geq n^2 - n. \tag{39}$$

We can use the above lower bound on the trace of $I - F$ to obtain a lower bound on the norm of the operator $I - F : \mathbf{L}(H) \to \mathbf{L}(H)$, where we consider $\mathbf{L}(H)$ with the Schatten 2-norm $\| \cdot \|_2$, defined in Appendix A. The Schatten 2-norm is the norm that arises from the trace inner product on $\mathbf{L}(H)$, also known as the Hilbert-Schmidt norm. We denote the corresponding operator norm on $\mathbf{L}(H) \to \mathbf{L}(H)$ by $\| \cdot \|_{2\to 2}$.

If F is self-adjoint as an operator on the space $\mathbf{L}(H)$ with the trace inner product, then from Lemma 3.7, we immediately obtain the bound

$$\|I - F\|_{2\to 2} \geq 1 - \frac{1}{n}. \tag{40}$$

In fact, the lower bound (40) is true for general unit-preserving abelian factorizable completely positive maps F. To see this, write $F = F_{\mathfrak{Re}} + i F_{\mathfrak{Im}}$ where both $F_{\mathfrak{Re}}$,

$F_{\mathfrak{Im}}$ are self-adjoint operators (not necessarily completely positive, however). Now

$$\operatorname{tr}_{\text{oper}}(I - F_{\mathfrak{Re}}) = \operatorname{tr}_{\text{oper}}(I - F) \geq n^2 - n. \tag{41}$$

Therefore

$$\|I - F\|_{2\to 2} \geq \|I - F_{\mathfrak{Re}}\|_{2\to 2} \geq 1 - 1/n. \tag{42}$$

In the discussion that follows, we need to consider another norm on the space $\mathbf{L}(H) \to \mathbf{L}(H)$ in addition to the norm $\|\cdot\|_{2\to 2}$ just considered. The new norm, which we denote $\|\cdot\|_{\infty\to\infty}$, is also an operator norm on $\mathbf{L}(H) \to \mathbf{L}(H)$, but relative to the $\|\cdot\|_\infty$ norm on $\mathbf{L}(H)$. The $\|\cdot\|_{\infty\to\infty}$ norm is different from the $\|\cdot\|_{2\to 2}$ norm, but for finite dimensional spaces H the two norms are equivalent, which means that each norm is bounded relative to the other. To obtain the bounding constants, note that if $T \in \mathbf{L}(H)$,

$$\|T\|_\infty \leq \|T\|_2 \leq \sqrt{n}\|T\|_\infty. \tag{43}$$

From this it follows that

$$\frac{1}{\sqrt{n}}\,\|F\|_{2\to 2} \leq \|F\|_{\infty\to\infty} \leq \sqrt{n}\,\|F\|_{2\to 2}. \tag{44}$$

which is the desired relative bound. In (40), if we substitute F by $I - F$, we immediately obtain the following proposition:

Proposition 3.8. *Suppose H is a Hilbert space of finite dimension n. If a unit-preserving completely positive map $F : \mathbf{L}(H) \to \mathbf{L}(H)$ has the form* (31)*, then*

$$\|I - F\|_{\infty\to\infty} \geq n^{-1/2}(1 - 1/n). \tag{45}$$

To prove the crucial result for the No-Go Theorem, we only use case $n = 2$ of (45).

Theorem 3.9. *Suppose H is of dimension ≥ 2. If F is a unit-preserving completely positive map on $\mathbf{L}(H)$ with an abelian factorization and $\beta < \sqrt{2}/4$, then*

$$\|U^\dagger T U - F(T)\|_\infty \geq \beta\ \|T\|_\infty \tag{46}$$

for at least one $T \in \mathbf{L}(H)$.

If H is finite dimensional, we can take $\beta = \sqrt{2}/4$.

Proof. Replacing F by the completely positive map $T \mapsto UF(T)U^\dagger$, we can assume without loss of generality that $U = I$. To prove this, we will show that the assertion that

$$\|T - F(T)\|_\infty < \beta\ \|T\|_\infty, \quad \forall T \in \mathbf{L}(H), \tag{47}$$

leads to a contradiction. However, (47) implies

$$\|I - F\|_{\infty\to\infty} \leq \beta. \tag{48}$$

We now reduce the proof to the case H has dimension 2, by considering a Hilbert space K of dimension 2 and completely positive unit-preserving mappings $Q : \mathbf{L}(K) \to \mathbf{L}(H)$ and $R : \mathbf{L}(H) \to \mathbf{L}(K)$ such that $R \circ Q$ is the identity map on $\mathbf{L}(K)$.

If I_H can be approximated to within β of the abelian factorizable F, then RFQ is also abelian factorizable and

$$\|I_K - RFQ\| = \|RI_HQ - RFQ\| \leq \|I_H - F\| \leq \beta < \sqrt{2}/4. \tag{49}$$

However, in this contradicts Proposition 3.8.

In the finite dimensional case, the norm is actually achieved so that in (48) the $\leq$ sign can be replaced by $<$ and so we can take $\beta \leq \sqrt{2}/4$ as claimed.[9] □

3.6. Proof of Encoding No-Go Theorem.

3.6.1. *Two Lemmas.*

LEMMA 3.10. *Suppose that* $\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$ *holds. If* $P : \mathbf{T}(H_{\text{comp}}) \to \mathbf{T}(H_{\text{comp}})$ *is* γ*-damped and* $\mathfrak{A}$ *and* $\mathbf{E}_{\mathfrak{A}}$ *are as identified in Lemma 3.3, then for every* $T \in \mathbf{L}(H_{\text{logical}})$,

$$\|\mathcal{M}_{\text{enc}}^{\text{t}} \mathbf{E}_{\mathfrak{A}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T) - U^{\dagger} T U\|_{\infty} \leq (2\gamma + \alpha)\|T\|_{\infty}. \tag{50}$$

PROOF. The $\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$ implies that for every $\rho \in \mathbf{T}(H_{\text{logical}})$ with $\|\rho\|_1 \leq 1$ and self-adjoint $T \in \mathbf{L}(H_{\text{logical}})$,

(51)
$$\left|\operatorname{tr}\left[\left\{\mathcal{M}_{\text{dec}}(P(\mathcal{M}_{\text{enc}}(\rho))) - U\rho U^{\dagger}\right\}T\right]\right| = \left|\operatorname{tr}\left[\rho\left\{\mathcal{M}_{\text{enc}}^{\text{t}}(P^{\text{t}}(\mathcal{M}_{\text{dec}}^{\text{t}}(T))) - U^{\dagger}TU\right\}\right]\right| \\ \leq \alpha\|T\|_{\infty}.$$

It follows that for every $T \in \mathbf{L}(H_{\text{logical}})$,

$$\|\mathcal{M}_{\text{enc}}^{\text{t}}(P^{\text{t}}(\mathcal{M}_{\text{dec}}^{\text{t}}(T))) - U^{\dagger}TU\|_{\infty} \leq \alpha\|T\|_{\infty}. \tag{52}$$

$\mathfrak{A}$ is commutative and by Lemma 3.3, for each $T \in \mathbf{L}(H_{\text{logical}})$

$$\|P^{\text{t}}(T) - \mathbf{E}_{\mathfrak{A}} P^{\text{t}}(T)\|_{\infty} \leq 2\gamma\|T\|_{\infty}. \tag{53}$$

Thus using the fact that $\mathcal{M}_{\text{dec}}$ and $\mathcal{M}_{\text{enc}}$ have norm ≤ 1, for every $T \in \mathbf{L}(H_{\text{logical}})$,

$$\begin{aligned} &\|\mathcal{M}_{\text{enc}}^{\text{t}} \mathbf{E}_{\mathfrak{A}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T) - U^{\dagger}TU\|_{\infty} \\ &\quad \leq \|\mathcal{M}_{\text{enc}}^{\text{t}} \mathbf{E}_{\mathfrak{A}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T) - \mathcal{M}_{\text{enc}}^{\text{t}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T)\|_{\infty} \\ &\quad + \|\mathcal{M}_{\text{enc}}^{\text{t}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T) - U^{\dagger}TU\|_{\infty} \\ &\quad \leq (2\gamma + \alpha)\|T\|_{\infty}. \end{aligned} \tag{54}$$

□

LEMMA 3.11. *If* H_{logical} *is of dimension* ≥ 2, *and* P, U, $\mathcal{M}_{\text{enc}}$, $\mathcal{M}_{\text{dec}}$ *and* $\mathbf{E}_{\mathfrak{A}}$ *are the same as in Lemma 3.10, and if* $\beta < \sqrt{2}/4$, *then for some non-zero* $T \in \mathbf{L}(H_{\text{logical}})$,

$$\|\mathcal{M}_{\text{enc}}^{\text{t}} \mathbf{E}_{\mathfrak{A}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}(T) - U^{\dagger}TU\|_{\infty} \geq \beta\|T\|_{\infty} \tag{55}$$

PROOF. The unit-preserving completely positive map $R = \mathcal{M}_{\text{enc}}^{\text{t}} \mathbf{E}_{\mathfrak{A}} P^{\text{t}} \mathcal{M}_{\text{dec}}^{\text{t}}$ factors through the abelian von Neumann algebra $\mathfrak{A}$; this follows from the presence of the projection operator $\mathbf{E}_{\mathfrak{A}}$ in the expression for R. Then (55) follows from Theorem 3.9. □

[9] We note that it is possible to derive explicit results as well for the case $n = 3$. In this case one can show that one obtains a larger numerical bound than $\sqrt{2}/4$, which applies when $\dim(H_{\text{logical}}) \geq 3$.

3.6.2. *Statement of Proof of Encoding No-Go Theorem.*

Proof. By the hypotheses of the Encoding No-Go Theorem (Theorem 3.2), the quantity $2\gamma+\alpha < \sqrt{2}/4$. Choose β such that $2\gamma+\alpha < \beta < \sqrt{2}/4$. From Lemma 3.10, it follows that for every $T \in \mathbf{L}(H_{\mathrm{logical}})$,

$$\|\mathcal{M}^{\mathrm{t}}_{\mathrm{enc}}\mathbf{E}_{\mathfrak{A}}P^{\mathrm{t}}\mathcal{M}^{\mathrm{t}}_{\mathrm{dec}}(T) - U^{\dagger}TU\|_{\infty} < (2\gamma+\alpha)\|T\|_{\infty}. \tag{56}$$

On the other hand by (55) in Lemma 3.11, there is a non-zero T such that

$$\|\mathcal{M}^{\mathrm{t}}_{\mathrm{enc}}\mathbf{E}_{\mathfrak{A}}P^{\mathrm{t}}\mathcal{M}^{\mathrm{t}}_{\mathrm{dec}}(T) - U^{\dagger}TU\|_{\infty} \geq \beta\|T\|_{\infty}. \tag{57}$$

Since $\|T\|_{\infty} > 0$, equations (56) and (57) imply $\beta \leq 2\gamma+\alpha$, which contradicts the choice of β. □

3.7. Interpretation of Encoding No-Go Theorem. The Encoding No-Go Theorem is an extremely powerful application of the QCC. With this theorem, one can calculate the amount of damping for which fault-tolerant quantum computation becomes impossible. When the amount of damping exceeds the critical amount, which means that the value of 2γ becomes less than the critical value $2\gamma_{\mathrm{critical}} = \sqrt{2}/4 - \alpha$, we find that the only solutions to the QCC are those for which dim $H_{\mathrm{logical}} = 1$. As noted above, in this case no meaningful quantum computation is possible, since not even one quantum bit can be accomodated.

In order to analyze the constraints on solutions to $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$ implied by the No-Go Theorem, we regard the pair $\{U, \alpha\}$ as given, since both the desired quantum computation U, and the maximum acceptable implementation inaccuracy α, are prescribed. We assume that U is defined on a Hilbert space H_{logical} such that $\dim(H_{\mathrm{logical}}) \geq 2$, to allow meaningful quantum computation. For practical applications, one then seeks to determine triples $\{P, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}\}$ that satisfy $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$. The No-Go Theorem, on the other hand, identifies conditions in which $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$ is not satisfied. Thus the No-Go Theorem provides a useful calculational tool for eliminating prospective quantum computer implementations that are guaranteed to fail. With the criterion provided by the No-Go Theorem, we can bound the space of solutions to $\mathbf{QCC}(P, U, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}, \alpha)$. This allows exploration of trade-offs amongst the members of the triple $\{P, \mathcal{M}_{\mathrm{enc}}, \mathcal{M}_{\mathrm{dec}}\}$, with which one may construct generalized "phase diagrams" that indicate boundaries between *potentially acceptable* and *definitely unacceptable* values for P, $\mathcal{M}_{\mathrm{enc}}$ and $\mathcal{M}_{\mathrm{dec}}$.

4. Quantum Components

4.1. Introduction. As defined in Section 2, we refer to a physically realizable device intended to implement a quantum computation as a *quantum component.* Mathematically, a quantum component is represented by a completely positive, trace preserving map, P. The detailed form of P, as an explicit function, is dictated by underlying equations of motion.

For a closed physical system, the quantum mechanical dynamics of the system are given by the Schrödinger equation associated to a particular Hamiltonian $\mathcal{H}$. However, for the general problem of a *practical* quantum computer, we must analyze realistic quantum components that interact with their environment, dissipate heat and exhibit decoherence. We must thus utilize a formulation that yields equations of motion appropriate to open quantum mechanical systems.

The connection to the Quantum Computer Condition presented in Section 2 is made by starting with the appropriate equations of motion that describe the dynamical evolution of a realistic quantum component interacting with its environment. One proceeds by solving the appropriate equations of motion. The explicit solution thus obtained provides the time-dependence of the quantum mechanical state of the open system. In principle, this allows us to deduce the explicit functional form of P.

Formulations of equations of motion for quantum components that interact with complex environments comprised of many degrees-of-freedom necessarily involve approximations of one sort or another, and there is not in general a unique choice. In this section we illustrate the general approach by making use of a Lindblad-type equation (made more precise below) to describe how one obtains the quantum component P that appears in the Quantum Computer Condition.

4.2. Dynamical Equations of Motion.

4.2.1. *Time-dependent generalization of the Lindblad equation.* The state of a quantum mechanical system defined on a Hilbert space H can be modeled by a density operator $\rho(t)$ whose time dependence obeys a linear (time dependent) equation

$$\frac{d}{dt}\rho(t) = A(t)\rho(t), \tag{58}$$

where $A(t)$ is an operator acting on $\mathbf{T}(H)$, the Banach space of trace class operators on H. For a closed system we have the Schrödinger equation, and the right-hand-side of (58) is given by

$$A(t)\rho = -\frac{i}{\hbar}[\mathcal{H}(t), \rho], \tag{59}$$

where the Hamiltonian $\mathcal{H}(t)$ is a self-adjoint operator which may depend on the parameter t.

However, it would be impractical to describe realistic quantum components using (59), since writing down the detailed Hamiltonian operator to account for all of the degrees-of-freedom comprising the quantum component and its environment would be intractable.

Motivated by the work of Lindblad [**21**], we make use instead of the following expression for the action of $A(t)$ on ρ:

$$A(t)\rho = -\frac{i}{\hbar}[\mathcal{H}(t), \rho] + \sum_j \left[L_j(t)\rho L_j^\dagger(t) - \frac{1}{2}\big\{L_j^\dagger(t)L_j(t), \rho\big\}\right] \tag{60}$$

where as above the $\mathcal{H}(t)$ is a self-adjoint operator which may depend on the parameter t, and the L_j are operators that describe effects arising from interaction with the environment, such as dissipation and decoherence. These operators are generalizations of the Lindblad operators of [**21**]; unlike the treatment given by Lindblad in [**21**], however, which considered only time-independent Hamiltonians $\mathcal{H}$ and time-independent dissipative perturbations L_j, with all operators bounded, we will allow unbounded and time-dependent $\mathcal{H}(t)$ and time-dependent (but still bounded) dissipative perturbations $L_j(t)$. Our treatment generalizes that given in [**21**], and we will refer to the equation of evolution

$$\frac{d}{dt}\rho(t) = -\frac{i}{\hbar}[\mathcal{H}(t), \rho] + \sum_j \left[L_j(t)\rho L_j^\dagger(t) - \frac{1}{2}\{L_j^\dagger(t)L_j(t), \rho\}\right] \tag{61}$$

as the *time-dependent generalization of the Lindblad equation.* As an example of how one may approximate the dynamics of a quantum component interacting with a complex environment, this equation provides a starting point to the derivation of P used in the Quantum Computer Condition. For this purpose we need to consider solutions to equations of the type given in (61) known as "fundamental solutions."

4.3. Fundamental Solutions. The concept of a *fundamental solution* associated to an evolution equation (see [**30**], §4.4) of the general form (58), such as (61) in particular, where ρ is a function with values in the Banach space $\mathbf{T}(H)$ and $A(t)$ is a one-parameter family of (possibly unbounded) linear operators on $\mathbf{T}(H)$, will play an important role in this paper. A *fundamental solution* associated to an equation of motion is a solution of an operator version of the original equation. We show below how, given a fundamental solution, one obtains the completely positive, trace preserving map P that appears in the Quantum Computer Condition.

Fundamental solutions are given by a family $\{P_{t,s}\}_{t\geq s\geq 0}$ of bounded operators on $\mathbf{T}(H)$ indexed on pairs of real numbers t and s satisfying equations

$$\frac{d}{dt}P_{t,s} = A(t)P_{t,s} \tag{62}$$

and

$$P_{s,s} = I. \tag{63}$$

The intended interpretation of $P_{t,s}$ is that if the system is in state ρ at time s, then the system will be in state $P_{t,s} \cdot \rho$ at later time t, that is

$$\rho(t) = P_{t,s} \cdot \rho(s). \tag{64}$$

4.3.1. *Existence and Positivity Properties of Fundamental Solutions.* The problem of the existence and uniqueness of fundamental solutions is a central one in the mathematical theory of evolution equations. In addition to addressing the question of the existence of fundamental solutions, it is important for our analysis to determine the positivity properties of fundamental solutions. This is because, as we shall see, the complete positivity of the map P that explicitly appears in the Quantum Computer Condition is inherited from the complete positivity of the set of fundamental solutions $\{P_{t,s}\}$. Positivity is important in ensuring that the set $\{P_{t,s}\}$, as well as P, carry density matrices to density matrices.

For equations of motion associated to finite dimensional systems, existence and uniqueness of solutions follows from the Lipschitz theorem on ordinary differential equations. Lindblad's analysis extended to infinite-dimensional (but bounded) systems, so, more generally, Lindblad characterized the infinitesimal generator of a *norm continuous* completely positive semigroup [**21**], which corresponds to the case of (58) in which $A(t)$ is constant and norm bounded (but possibly infinite-dimensional), *i.e.*, for the standard, time-independent Lindblad equation.

In order to generalize Lindblad's analysis to allow us to study infinite-dimensional, unbounded, time-dependent quantum systems, we will need to consider general evolution equations (58) in which $A(t)$ may be unbounded as well as time-dependent, for the infinite-dimensional case. The general theory of such equations was developed by Kato, Yosida and others in the 1950's. We will rely on results of Kato [**14**] which pertain to both existence of solutions and positivity properties, and on Theorem 4.4.1 of [**30**] which pertains to existence of solutions; moreover, we will use a constructive form of the theorem (which follows from an examination of the proof) which expresses the fundamental solution as a limit of a product of exponentials. The basic assumption of the approach is that if the $A(t)$ are generators with sufficiently smooth variation, then fundamental solutions exist.

Our system comprised of a quantum component interacting with its environment, described by (61), consists of a time-dependent Hamiltonian $\mathcal{H}(t)$ characterized by a time-dependent perturbation $V(t)$ of a (possibly unbounded) self-adjoint operator $\mathcal{H}_0$ so that we have $\mathcal{H}(t) = \mathcal{H}_0 + V(t)$. In order to apply Kato's theory for time dependent evolution equations, we will assume among other things that the perturbation $V(t)$ does not change the domain of $\mathcal{H}_0$. For the necessary background see ([**14**],[**30**]). We now state a proposition that asserts the existence and complete positivity of fundamental solutions to operator versions of the time-dependent generalization of the Lindblad equation given in (61):

Proposition 4.1. *For suitably regular time-varying potentials $V(t)$ and dissipation operators $L_j(t)$, there exists a strongly continuous completely positive operator $P_{t,s}$ which is a fundamental solution to the time-dependent generalization of the Lindblad equation.*

The exact statement of the conditions for the above in the form of a theorem, and proof, are given in Appendix B in §B.3 and §B.4.

4.4. Construction of Quantum Components. Having established the existence and complete positivity of fundamental solutions to the operator form of the underlying equation of motion for our system (comprised of the quantum component interacting with its environment), it is straightforward to obtain an expression for the completely positive, trace preserving map P, characterizing the quantum component, that explicitly appears in the QCC. This is simply obtained by noting (*cf* (64)) that the time-evolution of the state $\rho(t)$ between an initial fixed time $\hat{s}$ (corresponding to the start of the quantum computation) and a final fixed time $\hat{t}$ (corresponding to the end of the quantum computation) is fully specified by the fundamental solution defined with respect to those time values, $P_{\hat{t},\hat{s}}$, so that we have

$$\rho(\hat{t}) = P_{\hat{t},\hat{s}} \cdot \rho(\hat{s}), \tag{65}$$

and hence the completely positive, trace-preserving map P that appears in the QCC is given by the equivalence

$$P \equiv P_{\hat{t},\hat{s}} \ . \tag{66}$$

5. Unified Treatment of Quantum Computing Paradigms

5.1. Introduction. In this section we show that the QCC provides a unifying framework in which to describe on the same footing the currently-known "paradigms" for quantum computation, including the *circuit-based paradigm*, the *graph state-based paradigm*, the *adiabatic quantum computer paradigm.* The QCC subsumes all of these into a single, unifying paradigm for quantum computing.

5.2. Circuit-based paradigm. In this section we describe the specification of quantum components based on the "circuit-based" paradigm of quantum computation. We proceed as follows:

(1) For purposes of clarity, we begin in 5.2.1 by working in an idealization in which there is no noise present. For this idealized case we obtain the general form of the completely positive map P characterizing the quantum component. We then apply the result (for the noiseless idealization) to several specific realizations of the circuit-based paradigm. These include qubit-based quantum computers (these utilize states, the operators for which have a discrete eigenspectrum, *i.e.*, qubits in the case of 2-level systems), quantum continuous variable-based quantum computers (these utilize states, the operators for which have a continuous eigenspectrum, such as coherent states), and liquid state NMR-based quantum computers.

(2) Having obtained the general form for P in the noiseless case, for each of the three above-mentioned realizations of the circuit-based paradigm, we then explain in 5.2.2 how to modify the analysis, in a way appropriate to all choices of circuit realization, so as to account for the effects of noise.

5.2.1. *Idealized Circuits in the Absence of Decoherence and Dissipation.* A quantum circuit is described by a set G of gates operating in some specified order on elements of a set R of objects. The quantum states of these objects constitute the information which is "processed" by the gates of the quantum circuit. We associate with each object i of R a Hilbert space $H^{(i)}$ that describes the possible states of that particular object. The Hilbert space for the full set of objects on which the circuit operates is then

$$H_{\text{circuit}} = \bigotimes_{i \in R} H^{(i)} \ . \tag{67}$$

The gates in G, labeled by the index μ, are described by unitary operators $\hat{V}_\mu$, so that the unitary operator describing the (noiseless) operation of the circuit is

$$V_{\text{circuit}} = \prod_{\mu \in G} \hat{V}_\mu \ , \tag{68}$$

where the product of operations is ordered in accordance with the definition of the circuit. The factors $\hat{V}_\mu$ that appear in the multiplicand of (68) are in principle obtained from the fundamental solution to the appropriate underlying equation of motion, following the procedure outlined in Section 4 above.[10]

Each gate operates on a subset Σ_μ of the information elements, leaving the rest unaffected:

$$\hat{V}_\mu = V_\mu^{\Sigma_\mu} \otimes \Big(\bigotimes_{i \notin \Sigma_\mu} I_{H^{(i)}} \Big) \ , \tag{69}$$

[10] It is extremely important to note that we are *not* discussing here the abstractly defined quantum computation itself, which is prescribed in advance, and is represented by the unitary operator U that appears explicitly in the second term under the norm symbol in the QCC given in (12). Rather, we are discussing quantities that represent elements of a physical device that is to be used as an actual quantum computing machine. As such, the quantities under discussion here are to be regarded as "building blocks" for the *first* term under the norm symbol in (12).

where $I_{H^{(i)}}$ is the identity operator on $H^{(i)}$, and $V_\mu^{\Sigma_\mu}$ is the transformation effected by the μth gate, so that we may express the unitary operator describing the idealized circuit as

$$P \cdot \rho = V_{\text{circuit}} \rho V_{\text{circuit}}^\dagger \tag{70}$$

$$= \left(\prod_{\mu \in G} \hat{V}_\mu \right) \rho \left(\prod_{\mu \in G}{}' \hat{V}_\mu^\dagger \right) , \tag{71}$$

where the prime indicates that the second product reverses the order of the factors relative to the first product.[11]

Up to this point we have made no restrictions on the Hilbert spaces or the types of gates appearing in the specification of the circuit. We now describe three special cases of interest within the circuit-based paradigm: qubits, quantum continuous variables, and liquid state NMR. We obtain the completely positive, trace preserving map P that characterizes the implementation of the circuit for each example, thus showing that the QCC provides the proper foundational presentation of a quantum computer for all the cases.

(Case 1) *Circuit-realization with qubits*

The great majority of the research in quantum computation has focussed on circuits for which the information elements are qubits defined on a two dimensional Hilbert space $\mathbb{C}^2$, so that the full Hilbert space of the circuit is

$$H_{\text{circuit}} = \left(\mathbb{C}^2\right)^{\otimes |R|} . \tag{72}$$

where $|R|$ is the cardinality of the set of computational qubits.

Usually the set of gates is chosen from a relatively small set of operations, each of which acts on only 1 or 2 qubits. Specializing (69) to the case of a circuit built out of gates acting only on 1 or 2 qubits (this would be the proper description, for instance, of a machine that uses the universal set of quantum gates), we have

$$\hat{V}_\mu = V_\mu^{(i)} \otimes \bigotimes_{k(\neq i) \in R} I_k, \tag{73}$$

or

$$\hat{V}_\mu = V_\mu^{(ij)} \otimes \bigotimes_{k(\neq i,j) \in R} I_k . \tag{74}$$

where I_k is the identity operator acting on the copy of $\mathbb{C}^2$ associated to the kth qubit. With these definitions, the operator P that characterizes the implementation of the qubit-based realization of a quantum computer designed according to the circuit-based paradigm is given by (68) and (70). We thus see that the circuit-based paradigm, on which a large amount of the research in the field is based, is properly described by the QCC.

(Case 2) *Circuit-realization with quantum continuous variables*

[11] We strongly reiterate the message given in Footnote 10: It is only coincidentally the case that the form of (70) resembles that of (3). *Both* the right- and left-hand sides of (70) describe the physical device (*i.e.*, P), not the abstractly-defined quantum computation U, and thus both sides of eq.(70) are to be associated with the first term under the norm symbol in the QCC given in (12).

Alternatively, we may select different Hilbert spaces $H^{(i)}$ appropriate for quantum computation using quantum continuous variables (QCV). For instance, the $H^{(i)}$ might describe the states of simple harmonic oscillators. The full Hilbert space of the circuit, and the gate operations out of which it is built, are then defined analogous to the above prescriptions for the qubit-based quantum computer. In this way we arrive at a specification of the quantum component P appropriate to the case of computation by QCV. Thus, the QCV realization of the circuit-based paradigm is also seen to be properly described by the QCC.

(Case 3) *Circuit-realization with NMR states*

The treatment of quantum computation by nuclear magnetic resonance (NMR) in liquids requires special consideration due to the fact that the NMR sample effectively contains many copies of the circuit carrying out the same computation. In this case we define the Hilbert space of the system as

$$H_{\mathrm{NMR}} = H_{\mathrm{circuit}}^{\otimes N_s} \ , \tag{75}$$

where N_s is the number of copies of the circuit, which requires that we extend the definition of the unitary operation for the circuit as follows:

$$V_{\mathrm{NMR}} = V_{\mathrm{circuit}}^{\otimes N_s} \ . \tag{76}$$

We then obtain

$$P\rho = V_{\mathrm{NMR}} \rho V_{\mathrm{NMR}}^{\dagger} \tag{77}$$

which describes the NMR-based quantum computer in the QCC.[12]

5.2.2. *Quantum Circuits in the Presence of Decoherence and Dissipation.* Thus far in this section we have restricted ourselves to a discussion of quantum circuits in the absence of decoherence and dissipation. This is reflected in our description of the gates as implementing purely unitary operations, as in (68). Even at this level of description the circuit is not necessarily error-free. Unitary errors derive from a situation in which the evolution of the quantum circuit is unitary, but the circuit does not implement exactly the desired unitary computation:

$$V_{\mathrm{circuit}} \neq U \ . \tag{78}$$

Unitary errors can arise from either the design or the physical implementation of the circuit. Design errors arise, for example, due to the the fact that a universal set of quantum gates only allows for the implementation of an arbitrary unitary operation U to within an arbitrarily small tolerance [**23**]. In general there will then be some residual error implied by the very design of the circuit. Implementation errors result from inaccuracies in the physical parameters governing the unitary evolution associated with a gate as compared with the specification of those parameters by the design. For example, an interaction Hamiltonian may be applied for a longer time than specified, or there may be errors in the field strengths or couplings in the interaction Hamiltonian.

[12] In connection with (77) we repeat the admonition given in Footnote 11 .

In addition to unitary errors, we also need to deal with errors resulting from decoherence and dissipation. We will refer to these simply as decoherent errors.[13] In this case the gates are described by completely positive maps $\hat{P}_\mu$, where the hat on the P indicates that this quantum component is a single gate, and the index μ identifying the particular gate, as above. In addition to replacing unitary operations representing the gates by completely positive maps, it is also important to account for errors occurring in the transmission of quantum states from one gate to the next. This means that the transmission channels are also represented by completely positive maps designated by the symbol $\hat{P}_\mu$. In effect, the transmission channels (including any quantum memories used to store the states) are regarded as gates that (ideally) implement the identity transformation: $\hat{V}_\mu = I$. If we call the set of transmission channels C, the completely positive map that describes the circuit is then

$$P = \prod_{\mu \in G \cup C} \hat{P}_\mu \ , \tag{79}$$

where the index μ now identifies both the transmission channels (in C) and the gates (in G).

The operators $\hat{P}_\mu$ are obtained by explicitly solving the equations of motion for the physical device that implements the gate. The result may be written formally as the sum of two terms, one of which represents the action of the unitary operator $\hat{V}_\mu$ describing the ideal gate as specified by the circuit design, and the other of which represents the effects of unitary implementation errors as well as decoherence and/or dissipation:

$$\hat{P}_\mu \rho = (1 - \epsilon_\mu) \left(\hat{V}_\mu \rho \hat{V}_\mu^\dagger \right) + \epsilon_\mu \hat{Q}_\mu \rho \ , \tag{80}$$

where ϵ_μ is the probability that an error occurs during the operation of the gate, and $\hat{Q}_\mu$ is a completely positive map that represents the effects of the error. Although we have indicated how this follows in principle from an explicit solution of the detailed dynamics of the gate (as described in §4), an error model of this form is often assumed from the outset. The latter approach necessitates the choice of some specific operator $\hat{Q}_\mu$ to represent the errors. For instance, in investigating the properties of quantum error correcting codes one often invokes a "depolarization" qubit error model in which

$$\hat{Q}_\mu \rho \equiv \frac{1}{4} \left(\rho + \sum_{j=1}^{3} \sigma_j \rho \sigma_j \right) \ , \tag{81}$$

where the σ_j are the Pauli matrices acting on a single qubit. The advantage of this approach is that it abstracts the physical implementation of the quantum computer from the design of the circuit while retaining the main features of decoherence that must be addressed in the development of any practical quantum computer. The disadvantage is that the abstraction must then be justified relative to the detailed

[13] The case of liquid state NMR admits another type of error, which arises when the operators $\hat{V}^{(k)}_{\text{circuit}}$ appearing in (76) effect different unitary errors on different copies (k) of the circuit. These are known as incoherent errors.

physical implementation of the computer in order to apply rigrously the results of any analysis based on (81).

Whether we arrive at (80) by detailed calculation or by abstraction, we may use it in conjunction with (79) to describe the operation of the entire circuit:

$$P \cdot \rho = \left[\prod_{\mu} (1 - \epsilon_{\mu}) \right] V_{\text{circuit}} \rho V_{\text{circuit}}^{\dagger} + \left\{ 1 - \left[\prod_{\mu} (1 - \epsilon_{\mu}) \right] \right\} \epsilon_f Q_f \rho \ , \tag{82}$$

where Q_f incorporates the effects of the individual gate errors. We define an error probability associated with the entire circuit:

$$\epsilon_f \equiv 1 - \prod_{\mu} (1 - \epsilon_{\mu}) \ \ , \tag{83}$$

with which we have

$$P \cdot \rho = (1 - \epsilon_f) \, V_{\text{circuit}} \rho V_{\text{circuit}}^{\dagger} + \epsilon_f Q_f \rho \ . \tag{84}$$

We will make use of this error model in applying the QCC to the problem of finding error thresholds for fault tolerance in §6.

We note that eqs. (80) and (84) connect theoretical analysis with experimental observations. A general theoretical method for obtaining an explicit expression for the quantum component, P, in terms of the underlying equation of motion for the system, has been given above in §4. From an *experimental* perspective, explicitly writing (80) or (84) is a goal of quantum process tomography, which is by definition the experimental method of determining the evolution of open quantum systems [**33**].

5.3. Adiabatic Quantum Computing Paradigm. We now show that the QCC also provides the proper framework in which to formulate the adiabatic quantum computing paradigm. In adiabatic quantum computing, the quantum component can be described by a Lindblad equation incorporating a Hamiltonian of the form:

$$\mathcal{H}_{\text{adiabatic}} \, (t) = f \, (t) \, \mathcal{H}_0 + g \, (t) \, \mathcal{H}_f \tag{85}$$

where f and g are smooth functions of time with $f(0) = 1$, $f(T) = 0$, $g(0) = 0$ and $g(T) = 1$, so that the adiabatic Hamiltonian goes smoothly from $\mathcal{H}_0$ to $\mathcal{H}_f$ over time. The full Lindblad equation may then be written as

$$\frac{d}{dt} \rho(t) = -\frac{i}{\hbar} [\mathcal{H}_{\text{adiabatic}}(t) + \mathcal{V}(t), \rho] + \sum_j \left[L_j(t) \rho L_j^*(t) - \frac{1}{2} \{ L_j^*(t) L_j(t), \rho \} \right] \ , \tag{86}$$

where $\mathcal{V}(t)$ represents unitary errors and the terms involving $L_j(t)$ represent interactions with the environment.

The computation begins with an an initial preparation of the ground state of the Hamiltonian $\mathcal{H}_0$. Provided the conditions for adiabatic evolution are satisfied, evolution under the exact adiabatic Hamiltonian takes the ground state of $\mathcal{H}_0$ to the ground state of $\mathcal{H}_f$ with a high degree of accuracy. We identify the operator U that appears in the QCC as a unitary operator that describes this desired behavior:

$$U : |\phi_0\rangle \mapsto |\psi_0\rangle \ . \tag{87}$$

where $|\phi_0\rangle$ is the ground state of $\mathcal{H}_0$, $|\psi_0\rangle$ is the ground state of $\mathcal{H}_f$, and U is otherwise arbitrary.

The physical realization of the adiabatic quantum computer is described by (86), and thus implements the desired operation U only approximately. This is due to the approximation inherent in the adiabatic evolution itself, as well as any additional unitary errors, decoherence and dissipation. We express this fact quantitatively by using the fundamental solution of (86) to derive the map P (as described above in §4) that describes the operation of the adiabatic quantum component. The construction of the QCC then follows.

Note that the special case of the adiabatic quantum computer is characterized under $\mathbf{QCC}(P, U, \mathcal{M}_{\text{enc}}, \mathcal{M}_{\text{dec}}, \alpha)$ by two unique features:

(1) the encoding and decoding maps, $\mathcal{M}_{\text{enc}}$ and $\mathcal{M}_{\text{dec}}$ are identities, and
(2) the QCC is required to hold only for the ground state of the initial Hamiltonian, that is, for $\rho = |\phi_0\rangle\langle\phi_0|$.

5.4. Graph state-based (including cluster state-based) paradigm. We now consider the cluster-based approach to quantum computation ([**25**],[**26**], [**27**]), which is formulated in terms of an array of two level quantum systems. The systems in the array are referred to as sites and are elements of some set L which has a geometrical structure such as a 1 or 2 dimensional lattice; in addition to the geometrical structure there is also a flow structure which models the flow of information through the cluster. The two-dimensional Hilbert space corresponding to a site $\mathbf{s} \in L$ is denoted $H_{\mathbf{s}}$ and the Hilbert space H of the entire cluster system is the tensor product

$$H_{\mathbf{cluster}} = \bigotimes_{\mathbf{s}\in L} H_{\mathbf{s}}. \tag{88}$$

A key concept in the cluster approach is *measurement at a site* $\mathbf{s} \in L$ considered as an operation on quantum mechanical states. As an operation on pure states, the measurement corresponds to a pair of self-adjoint projections $E_{\mathbf{s}}$, $1 - E_{\mathbf{s}}$ on $H_{\mathbf{s}}$. In terms of the cluster system, we identify the projection $E_{\mathbf{s}}$ with a projection on $H_{\mathbf{cluster}}$ defined by

$$E = E_{\mathbf{s}} \otimes \bigotimes_{\mathbf{m}\neq\mathbf{s}} I_{H_{\mathbf{m}}} \tag{89}$$

where $I_{H_{\mathbf{m}}}$ is the identity operator acting on $H_{\mathbf{m}}$. The associated projective measurement on the cluster Hilbert space $H_{\mathbf{cluster}}$ is the completely positive map on density states[14]

$$P_E \cdot \rho = E\rho E + (1 - E)\rho(1 - E) \ . \tag{90}$$

The cluster scheme is illustrated in Figure 1.

A general class of cluster-type configurations associated to graphs has been introduced in the literature ([**27**], [**4**]). Given a graph $\mathcal{G} = (\mathbf{nodes}, \mathbf{edges})$, the lattice sites are the elements of **nodes**. Each lattice site $a \in \mathbf{nodes}$ has associated with it

[14] We note that the message of Footnote 11 applies to this equation.

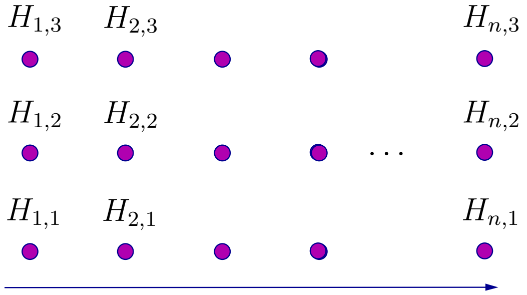

FIGURE 1. Two-dimensional cluster configuration (the arrow denotes time flow)

a two-dimensional Hilbert space H_a and an "entanglement" projection operator F that acts on the Hilbert space

$$H_{\mathbf{graph}} = \bigotimes_{a \in \mathbf{nodes}} H_a \tag{91}$$

as follows:[15] To each $(a, b) \in$ **edges**, define the projector of the form

$$\bigotimes_{n \in \mathbf{nodes} \setminus \{a,b\}} I_{H_n} \otimes F_{(a,b)}. \tag{92}$$

defined in terms of the Pauli matrices by

$$F_{(a,b)} = \frac{1}{2}\Big\{ I + \sigma_z^{(a)} + \sigma_z^{(b)} - \sigma_z^{(a)} \otimes \sigma_z^{(b)} \Big\}. \tag{93}$$

Then define

$$F = \prod_{(a,b) \in \mathbf{edges}} F_{(a,b)}. \tag{94}$$

F is a projection, since all the projectors $F_{a,b}$ pairwise commute.

5.4.1. *The Cluster Measurement Scheme.* In the cluster-based approach as explained in [**25**], a computation is realized by a sequence of projective measurements performed on different sites $\mathbf{s} \in L$. The projective measurement that is to be performed at each step of the computation is determined by a scheme that specifies at which site to make the measurement and what observable to measure at that site. These two choices depend on the outcome of the preceding measurements. In order to specify this process, a discrete time "flow" between the sites is also given. This flow determines the sequencing of sites to measure. It is important to note however that the specific projective measurement taken at each site depends on the outcome of the measurement taken at the preceding site.

At the level of specification, we can also consider the cluster measurement scheme as given by a multi-rooted tree $\mathbb{T}$. In Figure 2 we illustrate such a tree which because of spatial limitations is singly rooted. The tree consists of nodes and directed branches. Each node on the tree $\mathbb{T}$ corresponds to a pair $(\mathbf{s}, A)$ where $\mathbf{s} \in L$ is a cluster site and A is a two-level observable on $H_{\mathbf{s}}$. We will refer to $\mathbf{s}$ as the cluster site corresponding to the tree node $(\mathbf{s}, A)$. Each node $\ell = (\mathbf{s}, A)$ of the

[15] Such operators are considered from the more general point of view as partial isometries below in Definition 5.2 and in the discussion preceding it.

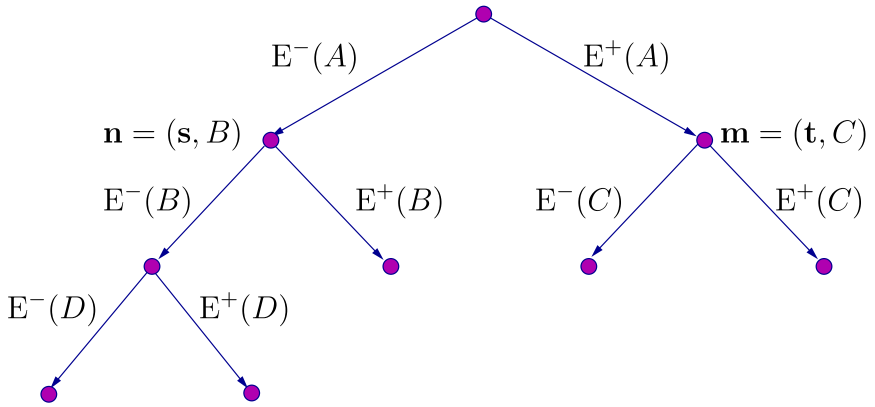

Figure 2. Example scheme of a cluster computation

tree has two outgoing branches corresponding to the two possible outcomes of the measurement of A. These two branches correspond to the spectral projections of A, which we denote $\mathrm{E}^+(A)$, $\mathrm{E}^-(A)$.

It is important to note that many different nodes of $\mathbb{T}$ may correspond to the same cluster site, that is two distinct computation sequences may take us to the same node but at which different measurements are taken. In fact, in the usual cluster approach all computation sequences traverse the exact same cluster nodes. This means that at each horizontal level of the tree $\mathbb{T}$, the nodes all have the same cluster site. In the general scheme outlined above, no such restriction exists. Thus we may consider schemes in which not only the subsequent measurement depends on previous outcomes, but in which the site at which the measurement is taken also dependent on previous outcomes.

For clusters that are not arranged in a 1 dimensional array, we can avoid the use of multiply rooted trees if we allow cluster systems that are not restricted to two-level systems. This means that the Hilbert space $H_{\mathbf{s}}$ corresponding to a site $\mathbf{s} \in L$ can have arbitrary dimension. In that case, the corresponding node observables are allowed to have more than two outcomes and in particular, the specification tree may not be binary.

A complete path (that is one which originates at the root node and terminates at a leaf node) of $\mathbb{T}$ is specified by a sequence of measurement outcomes, where the observable measured is associated to a node of the tree. Mathematically, each measurement outcome is expressed by one of the spectral projections associated to the measurement and graphically represented by an edge of the tree. A complete measurement outcome associated to a path is a sequence of projections, where each projection corresponds to a traversal of an edge of the tree as follows:

$$\ell_0 \xrightarrow{\mathrm{E}_0^\pm} \ell_1 \xrightarrow{\mathrm{E}_1^\pm} \ell_2 \xrightarrow{\mathrm{E}_2^\pm} \ell_3 \xrightarrow{\mathrm{E}_3^\pm} \cdots \xrightarrow{\mathrm{E}_k^\pm} \ell_{k+1}. \tag{95}$$

The projective measurement associated to the cluster consists of the projective measurements on sites following the branches of the cluster scheme tree. We can explicitly write this down:

Theorem 5.1. *The projective measurement on a cluster is of the form*

$$P_{\mathbb{T}} \cdot \rho = \sum_{\mathcal{P} \in \mathrm{Path}\mathbb{T}} \left(\prod_{\tau \in \mathcal{P}} E_\tau \right) \rho \left(\prod_{\tau \in \mathcal{P}} E_\tau \right) \tag{96}$$

where E_τ is a projector on the cluster site corresponding to the edge of the cluster scheme tree. Note that for each $\mathcal{P} \in \mathrm{Path}(\mathbb{T})$, all the E_τ with $\tau \in \mathcal{P}$ commute.

5.4.2. *Quantum Components in the graph state-based paradigm.* We now show that the graph state-based paradigm of quantum computation is properly described by the QCC. The paradigm has been described in the literature as employing an entangled substrate upon which a series of conditional projective measurements is performed. The projective measurements are used to carry out a computational algorithm, but can also be used to read input from a macroscopically observable input register or output to a macroscopically observable output register. The entangled substrate corresponds to some particular Hilbert subspace of entangled vectors which may be characterized in various ways, for instance as the range of an entangling operation or as the solutions to some eigenvalue equations.

Correspondingly, we should expect that the mathematical formulation of the graph model of a quantum component also consist of two parts (We assume as given the Hilbert space $H_{\mathbf{graph}}$):

(1) An initial "entanglement producing" operation of some kind.
(2) The projective measurement on $H_{\mathbf{graph}}$ corresponding to the graph scheme.

In our approach, we have already discussed how to formalize the step (2) above. However, there are several choices for the entanglement generating step (1). In the examples discussed in the literature, these are given by a self-adjoint projection operator, but it is natural from our viewpoint to consider more generally partial isometries $V : H \to H$.

Definition 5.2. A *graph state-based quantum component* $\mathcal{C}$ is a pair $(V, \mathbb{T})$ given by a cluster scheme $\mathbb{T}$ and an "entanglement" partial isometry V on H_{graph}. The completely positive map associated to $\mathcal{C}$ is defined by

$$Q_{\mathcal{C}} \cdot \rho = \sum_{\mathcal{P} \in \mathrm{Path}(\mathbb{T})} E_{\mathcal{P}} V \rho V^\dagger E_{\mathcal{P}} \tag{97}$$

Thus, we see that, just as for the circuit-based paradigm and the adiabatic quantum computing paradigm, the QCC provides an over-arching framework in which to formulate the graph-state based paradigm of quantum computing. Moreover, in this section we have generalized the definition of graph state- (and cluster state-) based quantum computers that has previously appeared in the literature. Our generalization consists of two features: (1) our definition allows for *arbitrarily different* measurements to be carried out at different nodes at the same level of the multi-rooted tree $\mathbb{T}$, and (2) our definition replaces the use of a self-adjoint projection operator as an entanglement generator with the more general notion of a partial isometry (which includes self-adjoint projections as a special case).

6. Error Thresholds and Fault Tolerance

6.1. Introduction. In §2.3.3 we showed that the recently discovered approach to error correction known as "operator quantum error correction" is in fact a special case of the general QCC formulation. Given the general applicability of the QCC to all quantum computing paradigms (*cf* §5), as well as to all techniques for protection against errors (including quantum error correction, decoherence-free subspaces and noiseless subsystems), the QCC thus provides a unified framework for a fully general analysis of fault tolerance in quantum computing. We refer to this as operator quantum fault tolerance (OQFT).

As an example of OQFT, in this section we describe the application of the QCC to the analysis of error thresholds for fault tolerance in the circuit paradigm. To make contact with previous research, we begin by discussing this subject from the perspective of the well established method based on the analysis of error probabilities [**28**], [**1**], [**15**], [**16**], [**24**], [**2**]. Since the QCC in fact provides the underlying framework in which to study any issues associated with physical quantum computation, we then reformulate the problem in terms of the QCC. This allows us to relate the results of the two approaches, and to determine the extent to which the previously utilized approach (based on the method of error probabilities) is in fact justified based on the insight provided with the QCC.

6.2. The Method of Error Probabilities. In this section we briefly describe the method of error probabilities. We begin by identifying a quantum operation that we wish to implement and specifying a circuit that (ideally) implements the operation. We then identify an error model for the gates in the circuit that accounts for the inevitable effects of dissipation and decoherence that come into play when the gates are implemented with real devices. By hypothesis, the probability that an error occurs in this "direct" implementation of the operation is too high for it to be useful as a component in a quantum computer.

In order to render the circuit more fault tolerant, we specify a second, more complicated, circuit using quantum error correction. The circuit now operates on the set of *encoded* qubits obtained by encoding the *logical* qubits of the direct implementation using a QECC. The gates in the original circuit are replaced by collections of gates that operate on the encoded qubits. Additional gates are added to carry out the QECC's recovery procedure wherever an error is detected. The error model is then applied to the gates in this new circuit. The error correction clearly provides some degree of protection against errors, but it also necessitates a larger number of gates, so that there are then more opportunities for errors to occur. In order to determine whether this procedure has improved the fault tolerance, we compare the probability of an uncorrected error occurring during operation of the QECC version (ϵ_f^{QECC}) with the probability of any error occurring in the "direct" implementation ($\epsilon_f^{\text{direct}}$). If the QECC error probability is smaller, that is, if

$$\frac{\epsilon_f^{\text{QECC}}}{\epsilon_f^{\text{direct}}} < 1 \ , \tag{98}$$

then the procedure has been at least partially successful. If the error probability of the new circuit is still too high, we can reduce the error probability further by concatenating the code, that is by encoding the qubits used in the QECC version using the same QECC and by redesigning the circuit to handle the second level of encoded qubits. By repeating the process of concatenation we can arrange that the error probability be made arbitrarily small.

The key point is that (98) can be shown to hold only if the failure probabilities of the individual gates are less than some threshold value that depends on the relative complexity of the encoded *vs.* un-encoded versions of the circuit. The thresholds appearing in these conditions are known as "error thresholds." If the threshold conditions are satisfied, then the use of concatenated codes will provide fault tolerant operation to within some specified tolerance. The problem of achieving fault tolerant quantum computation is reduced to the problem of constructing implementations of the primitive gates that satisfy the error threshold conditions.

6.3. Operator Quantum Fault Tolerance and the QCC. We now reconsider the above problem from the perspective of OQFT by making use of the QCC. Our goal is to identify a quantum component P, that implements (approximately) a quantum computation, U, that is, we write the quantum computer condition, $\mathbf{QCC}(P, U, \mathcal{M}_{\rm enc}, \mathcal{M}_{\rm dec}, \alpha)$,

$$\|\mathcal{M}_{\rm dec}(P \cdot (\mathcal{M}_{\rm enc}(\rho))) - U\rho U^\dagger\|_1 \leq \alpha \tag{99}$$

for some suitable choice of encoding and decoding maps, $\mathcal{M}_{\rm enc}$ and $\mathcal{M}_{\rm dec}$. For simplicity of notation we define an operator

$$\tilde{P} \equiv \mathcal{M}_{\rm dec} \cdot P \cdot \mathcal{M}_{\rm enc} \ , \tag{100}$$

so that the QCC becomes

$$\|\tilde{P}\rho - U\rho U^\dagger\|_1 \leq \alpha \ . \tag{101}$$

We begin by developing a "zero-th order" implementation that does not use a QECC. In the absence of errors, we assume that the implementation faithfully implements the computation U:

$$\tilde{P}^{(0)}\rho = \mathcal{M}_{\rm dec}\left[V^{(0)}_{\rm circuit}\left(\mathcal{M}_{\rm enc}\rho\right)V^{(0)\dagger}_{\rm circuit}\right] = U\rho U^\dagger. \tag{102}$$

With the error model (84) we have

$$\|\tilde{P}^{(0)}\rho - U\rho U^\dagger\| = \left\|\left(1-\epsilon^{(0)}_f\right)\mathcal{M}_{\rm dec}\left[V^{(0)}_{\rm circuit}\left(\mathcal{M}_{\rm enc}\rho\right)V^{(0)\dagger}_{\rm circuit}\right] + \epsilon^{(0)}_f\tilde{Q}^{(0)}_f\rho - U\rho U^\dagger\right\|_1 , \tag{103}$$

where, for generality, we have subsumed the encoding and decoding maps into the definition of $\tilde{Q}_f$. (The maps are identities for the zero-th order circuit.) With (102) the left hand side of the QCC takes the simple form

$$\|\tilde{P}^{(0)}\rho - U\rho U^\dagger\| = \epsilon^{(0)}_f\|\tilde{Q}^{(0)}_f\rho - U\rho U^\dagger\|_1 \ . \tag{104}$$

Note from (83) that the failure probability for this circuit is, to lowest order, linear in the error probabilities for the gates which make up the circuit:

$$\epsilon^{(0)}_f \sim \mathcal{O}\left(\epsilon_\mu\right) \ , \tag{105}$$

(recall that ϵ_μ represents gate error, *cf* (83)) a fact which, as we shall see, is crucial to the derivation of an error threshold.

We next construct the "first order" implementation of U, which operates in the codespace of the QECC. By the preceding arguments, this implementation will satisfy

$$\|\tilde{P}^{(1)}\rho - U\rho U^{\dagger}\| = \epsilon_f^{(1)} \|\tilde{Q}_f^{(1)}\rho - U\rho U^{\dagger}\|_1 \ . \tag{106}$$

Following [**24**], we consider the case that errors affect the qubits in the circuit independently and that the QECC recovery procedure is sufficient to correct a single error in any one qubit. In that case, the encoded circuit will exhibit an unrecoverable error only if two or more single qubit errors occur. In this case, the error probability will be quadratic in ϵ_μ to leading order:

$$\epsilon_f^{(1)} \sim \mathcal{O}\left(\epsilon_\mu\right)^2 \ . \tag{107}$$

At this point, the QECC has not eliminated all errors, but has resulted in a circuit with error probabilities that are quadratic, rather than linear, in the error probabilities of the primitive operations.

We have now introduced two implementations of the computation. If either implementation satisfies the QCC, then there is no need to continue. If the implementations do not satisfy the QCC, then it is meaningful to ask whether this can be achieved by concatenating the code. In order to answer this question, we begin by asking another, related question: has the QECC improved the fault tolerance of the implementation relative to the QCC? In other words, we wish to know under what conditions it is true that for all ρ

$$\|\tilde{P}^{(1)}\rho - U\rho U^{\dagger}\|_1 < \|\tilde{P}^{(0)}\rho - U\rho U^{\dagger}\|_1 \ , \tag{108}$$

or alternatively[16]

$$\sup_\rho \frac{\|\tilde{P}^{(1)}\rho - U\rho U^{\dagger}\|_1}{\|\tilde{P}^{(0)}\rho - U\rho U^{\dagger}\|_1} < 1 \ . \tag{109}$$

Using (104) and (106), this becomes

$$\sup_\rho \frac{\epsilon_f^{(1)}}{\epsilon_f^{(0)}} \cdot \frac{\|Q_f^{(1)}\rho - U\rho U^{\dagger}\|_1}{\|Q_f^{(0)}\rho - U\rho U^{\dagger}\|_1} < 1 \ . \tag{110}$$

The above equation represents the extension of (98) to OQFT obtained by using the general framework provided by the QCC. Clearly it does not reduce to a simple ratio of error probabilities, as in (98) above. The reason for this is that this formulation of the error threshold problem based on the QCC takes into account not only error probabilities, ϵ_f, but also expressions involving the norms of operators that characterize the "strength" of the errors. To see this, note that we began by assuming an error model represented by the operation $\tilde{Q}_f^{(0)}$ for the zero-th order implementation. The error model in the encoded implementation is represented, in general, by a different operation, $\tilde{Q}_f^{(1)}$. There is no reason to suppose that these

[16] Relation (109) is actually a stronger condition than (108) for infinite-dimensional vector spaces.

error models are equally effective in perturbing the computation. This is reflected in the difference in the norms:

$$\|\tilde{Q}_f^{(1)}\rho - U\rho U^\dagger\|_1 \neq \|\tilde{Q}_f^{(0)}\rho - U\rho U^\dagger\|_1 \ . \tag{111}$$

To further emphasize this point, we obtain the above result (98) based on the assumption that the error models are "commensurate" in the sense that

$$\|\tilde{Q}_f^{(1)}\rho - U\rho U^\dagger\|_1 \approx \|\tilde{Q}_f^{(0)}\rho - U\rho U^\dagger\|_1 \ . \tag{112}$$

We shall shortly return to the question of whether this is a good approximation. With this assumption, the condition (110) then becomes

$$\frac{\epsilon_f^{(1)}}{\epsilon_f^{(0)}} \lesssim 1 \ , \tag{113}$$

which is identical to the result (98) obtained by the method of error probabilities. We obtain the form of the error threshold by noting from (105) and (107) that the numerator and denominator of (113) are, to lowest order, quadratic and linear, respectively, in ϵ_μ, so that

$$\frac{\epsilon_f^{(1)}}{\epsilon_f^{(0)}} = \frac{\sum_{\mu\nu} A_{\mu\nu}\epsilon_\mu\epsilon_\nu + \cdots}{\sum_\mu B_\mu \epsilon_\mu + \cdots} \ . \tag{114}$$

At this point, it is straightforward to obtain a threshold if we set the ϵ_μ equal to each other, and take $\epsilon \equiv \epsilon_\mu$. Then one obtains the error threshold comparable to those obtained in [**24**], [**13**], [**35**], as

$$\epsilon \lesssim \frac{\sum_\mu B_\mu}{\sum_{\mu\nu} A_{\mu\nu}} \ . \tag{115}$$

The desired behavior of the concatenated QECC described above follows if we successively apply the approximation (112) at each level of concatenation:

$$\|\tilde{Q}_f^{(i+1)}\rho - U\rho U^\dagger\|_1 \approx \|\tilde{Q}_f^{(i)}\rho - U\rho U^\dagger\|_1 \ . \tag{116}$$

We note that Aliferis, Gottesman and Preskill [**2**] also relate the ratio of error probabilities for successive levels of concatenation to an overall measure of the "accuracy" of the quantum computation. Their approach differs from the one described here in three important ways:

(Contrast 1) Accuracy in [**2**] is defined in terms of the probabilities p_i of the outcomes i of measurements on the final output state for an ideal, as compared with a noisy, circuit:

$$\sum_i |p_i^{\text{noisy}} - p_i^{\text{ideal}}| \ . \tag{117}$$

In contrast, we define the accuracy of the implementation by the QCC.

(Contrast 2) The threshold proofs in [**2**] rely on proofs that the implementations at each level of concatenation are conditionally correct relative to the noise model. In this case the ratio of error probabilities $\epsilon^{(i+1)}/\epsilon^{(i)}$ is automatically the quantity

of interest in comparing performance at each level of concatenation. Here, in contrast, the QCC provides the figure of merit at each level of concatenation, and the dependence on error probabilities is inferred.
(Contrast 3) As a consequence of the two preceding points, [**2**] makes contact with the notion of accuracy only at the highest level of concatenation, at which the entire quantum component may be viewed as a black box. Here, the QCC is applied systematically at each level of concatenation.

At this point we have shown that we can obtain the standard form of the error threshold result from the QCC by introducing the assumption (116) on the relative strengths of the error models appropriate to successive levels of concatenation of the QECC. We now investigate the validity of the approximation. We begin by making some reasonable assumptions about the error operators and the initial state of the computer. We note that the operators $\tilde{Q}_f^{(i)}$ are trace preserving, and thus describe the evolution of the quantum component if a failure has in fact occurred, as can be seen by setting $\epsilon_f = 1$ in (84). It is then reasonable to expect that the state resulting from its operation on ρ will be "close" to the maximum entropy state[17] in the sense that, for small δ_p,

$$\|\tilde{Q}_f^{(i)}\rho - \rho_I\|_p < \delta_p \ , \tag{118}$$

where ρ_I is the maximum entropy state, and the value of p identifies the Schatten p-norm associated to the corresponding Schatten p-class (*cf* (126)).
On the other hand, it is normally the case that the input state for the quantum computation is a pure state, and thus so is the state $U\rho U^\dagger$. In this case, it is straightforward to show that

$$\|\rho_I - U\rho U^\dagger\|_1 = 2 - \frac{2}{N} \tag{119}$$

and

$$\|\rho_I - U\rho U^\dagger\|_\infty = 1 - \frac{1}{N} \ , \tag{120}$$

where N is the dimension of H_{logical}. Since

$$\|\tilde{Q}_f^{(i)}\rho - U\rho U^\dagger\| = \| \left[\tilde{Q}_f^{(i)}\rho - \rho_I\right] + \left[\rho_I - U\rho U^\dagger\right] \| \ , \tag{121}$$

we have, by triangle inequalities,

$$2 - \frac{2}{N} - \delta_1 \leq \|\tilde{Q}_f^{(i)}\rho - U\rho U^\dagger\|_1 \leq 2 - \frac{2}{N} + \delta_1 \tag{122}$$

or

$$1 - \frac{1}{N} - \delta_\infty \leq \|\tilde{Q}_f^{(i)}\rho - U\rho U^\dagger\|_\infty \leq 1 - \frac{1}{N} + \delta_\infty \tag{123}$$

[17] Note that this is not a good assumption for errors that operate locally on only one qubit in a larger set of qubits, leaving the others unaffected. This important case is a topic for further study.

where we have assumed implicitly that $N \gg 1$ and $\delta_p \ll 1$. Since these expressions hold for any value of i, (116) is a reasonable approximation with either choice of norm under the conditions that

(1) (118) holds for some $\delta_p \ll 1$, and
(2) the initial state of the computation is a pure state.

7. Conclusions

In this paper we have presented a fundamental, unifying framework for describing physically-realizable quantum computing machines. This is concisely stated in the form of the Quantum Computer Condition (QCC), an inequality that incorporates a complete specification of the full dissipative, decohering dynamics of the actual, practical device used as the quantum computing machine, a specification of the ideally-defined quantum computation intended to be performed by the machine, and a quantitative criterion for the accuracy with which the computation must be executed.

With the QCC we prove the fundamental Encoding No-Go Theorem that identifies the amount of damping (including dissipative and decohering effects) for which physically-realizable fault-tolerant quantum computing is not possible. We provide a rigorous definition of damping, and explicitly calculate a *universal* critical damping value for fault-tolerant quantum computation. This theorem can be used in principle to solve practical problems involving quantum computer design.

In this paper we have also presented an existence proof for fundamental solutions to useful classes of *time-dependent* generalizations of the Lindblad equation. This can provide a useful tool in analyzing a wide variety of open quantum mechanical systems.

We have demonstrated that the entire formalism of operator quantum error correction (OQEC) can be obtained from the QCC as a special case. By allowing for the possibility of residual errors, the general formalism of the QCC enables us to generalize OQEC to "operator quantum fault tolerance" (OQFT). Since we have demonstrated that OQEC is in fact a particular reduction of the QCC, and since standard quantum error correction (QECC), decoherence-free subspaces (DFS) and noiseless subsystems are all special cases of OQEC, we have discovered that QCC applies in general across *all* these approaches.

As an initial application of the OQFT concept, we have begun the exploration of the application of QCC to the problem of establishing thresholds for fault-tolerant quantum computation by showing that the standard approaches to this problem can be motivated within the framework of the QCC.

Research in quantum information science has resulted in the discovery of seemingly different *paradigms* for quantum computation, including the circuit-based paradigm, graph state-based paradigm and adiabatic quantum computing paradigm. In this paper we have explicitly demonstrated that these paradigms are not in fact distinct at a fundamental level, but are all describable within the unifying framework provided by the QCC. In the particular case of the graph state-based paradigm (which includes cluster state-based models), we not only show that the paradigm is a manifestation of the unifying picture provided by the QCC, but also introduce a definition of graph state-based quantum computers that generalizes the graph state models previously defined in the literature.

Future work motivated by our results should include applications of the Encoding No-Go Theorem to diverse problems pertaining to practical quantum computer design and implementation. It would also be of interest to further explore the physics of the operator quantum fault tolerance (OQFT) generalization of OQEC presented in this paper. Specific work along theses lines should include further application of the QCC to obtaining error thresholds for fault-tolerant implementations of quantum computers. It would also be fruitful to explore applications of the quantum computer condition to situations in which quantum process tomography techniques are used to experimentally characterize the quantum component described by the completely positive map that appears in the QCC.

Acknowledgements
We wish to thank Anthony Donadio and Yaakov Weinstein for helpful comments. This work was supported by MITRE under the MITRE Technology Program.

Appendix A. Banach Spaces of Operators

A linear map T on a Banach space is a *contraction* iff its norm is ≤ 1.

Let H be a separable Hilbert space. $\mathbf{L}(H)$ denotes the space of bounded operators on H with the operator norm, $\mathbf{K}(H)$ denotes the normed closed subspace of compact operators of $\mathbf{L}(H)$. In case H is finite dimensional, these spaces are identical. Assume now H is infinite dimensional; we consider other Banach spaces of compact operators defined by eigenvalue decay conditions and whose norms reflect the rate of decay of the eigenvalues. Specifically, let $T \in \mathbf{K}(H)$, then $|T| = \sqrt{T^\dagger T}$ is a non-negative compact operator and so by the spectral theorem, has a complete set of eigenvectors with eigenvalues that can be ordered in a sequence

$$s_0(T) \geq s_1(T) \geq \cdots \geq s_n(T) \geq 0 \tag{124}$$

which converges to 0. The following properties are well-known (see [**12**]; also [**7**] on which this discussion is based).

$\mathbf{T}(H)$ is the Banach space of trace-class operators T on H with the norm

$$\|T\|_1 = \sum_{k=0}^{\infty} |s_k(T)| \tag{125}$$

More generally, the Schatten p-class $\mathbf{T}_p(H)$ is defined by the condition

$$\|T\|_p = \left\{ \sum_{k=0}^{\infty} s_k(T)^p \right\}^{\frac{1}{p}} < \infty \tag{126}$$

with the norm given by $\|\cdot\|_p$. The operator norm for any $T \in \mathbf{L}(H)$, denoted by $\|T\|_\infty$, is defined as the supremum of $\|Tx\|$ for $x \in H$ of norm ≤ 1. If $T \in \mathbf{K}(H)$, the operator norm is also the supremum of the eigenvalues of $|T|$.

Appendix B. Completely Positive Maps and Fundamental Solutions

In the following, H denotes a complex Hilbert space. We will consider various Banach spaces of bounded operators on H: these are discussed in Appendix A above.

We will consider completely positive maps on both $\mathbf{L}(H)$ on the Schatten classes $\mathbf{T}_p(H)$ and especially on the trace-class operators $\mathbf{T}(H) = \mathbf{T}_1(H)$.

The basic fact about completely positive maps we use is the *Kraus representation*.

Proposition B.1. *A $P : \mathbf{T}(H) \to \mathbf{T}(H)$ is a completely positive contraction if and only if it is of the form*

$$P(\rho) = \sum_{i \in I} X_i \rho X_i^\dagger \tag{127}$$

where $X_i \in \mathbf{L}(H)$ with

$$\sum_i X_i^\dagger X_i \leq 1 \tag{128}$$

We will consider only *trace preserving* completely positive maps P, that is which satisfy

$$\operatorname{tr}(P(\rho)) = \operatorname{tr}(\rho) \tag{129}$$

Proposition B.2. *Suppose P is a completely positive map given by the Krauss form* (127)*.*

(1) *A necessary and sufficient condition P be trace-preserving is that*

$$\sum_{i \in I} X_i^\dagger X_i = 1. \tag{130}$$

(2) *A necessary and sufficient condition that P be bounded in the operator norm is that*

$$\sum_{i \in I} X_i X_i^\dagger \in \mathbf{L}(H). \tag{131}$$

Note that if T is a completely positive trace-preserving and operator norm continuous map, then by interpolation T is also norm continuous on the Schatten p-classes.

Proposition B.3. *If P is a completely positive trace-preserving map, then the adjoint of P on $\mathbf{L}(H)$ defined by*

$$\operatorname{tr}(P^{\mathrm{t}}(T)\rho) = \operatorname{tr}(T P(\rho)) \tag{132}$$

is a unit preserving completely positive map $\mathbf{L}(H) \to \mathbf{L}(H)$. Its Kraus representation is

$$P^{\mathrm{t}}(T) = \sum_{i \in I} X_i^\dagger T X_i \tag{133}$$

Note that the completely positive unit preserving maps $\mathbf{L}(H) \to \mathbf{L}(H)$ which are adjoints of completely positive trace-preserving maps on $\mathbf{T}(H) \to \mathbf{T}(H)$ can be characterized precisely as those which are continuous mappings $\mathbf{L}(H) \to \mathbf{L}(H)$, where $\mathbf{L}(H)$ has the ultraweak topology.

B.1. Completely Positive Semigroups on $\mathbf{T}(H)$. We need to first establish that each generalized Lindblad-type operator $A(t)$ (*cf* eqs.(58) and (60)) generates a semigroup of completely positive contractions on $\mathbf{T}(H)$ *with respect to the trace-class norm* $\| \cdot \|_1$. We will also consider boundedness properties relative to the operator norm $\| \cdot \|_\infty$, although in general the corresponding semigroups may not be contraction semigroups in this norm.

We begin with a general result characterizing infinitesimal generators of strongly continuous positive (or completely positive) semigroups on the Banach space $\mathbf{T}(H)$. Recall that a one-parameter semigroup $\{T_t\}_{t\geq 0}$ on a Banach space E is said to be of class C_0 iff for every $x \in E$, $\lim_{t\to s} T_t(x) = T_s(x)$. If $\{T_t\}_{t\geq 0}$ is a C_0-semigroup, then there are positive constants M and β such that

$$\|T_t\| \leq M e^{t\beta}. \tag{134}$$

Moreover,

$$Ax = \lim_{h\to 0} h^{-1}(T_h x - x) \tag{135}$$

is a densely-defined operator called the *infinitesimal generator* of $\{T_t\}_{t\geq 0}$

Theorem B.4. *Suppose A is a densely-defined operator on $\mathbf{T}(H)$ which generates a contractive semigroup $\{T_t\}_{t\geq 0}$ on $\mathbf{T}(H)$. A necessary and sufficient condition the operators $\{T_t\}_{t>0}$ be positive (respectively completely positive) is that for each $\lambda > 0$*

$$\mathrm{R}(\lambda, A) = (\lambda I - A)^{-1} \tag{136}$$

(which is defined by the Hille-Yosida Theorem) be positive (respectively completely positive). The operators T_t are trace-preserving iff in addition for all $\lambda > 0$,

$$\mathrm{tr}(\mathrm{R}(\lambda, A)\rho) = \lambda^{-1}\,\mathrm{tr}(\rho) \tag{137}$$

for every $\rho \in \mathbf{T}(H)$.

The family of operators $\{T_t\}_{t>0}$ extends to a C_0-semigroup on $\mathbf{L}(H)$ iff there are constants M' and β' such that for all $\lambda > \beta'$ and for all $\rho \in \mathbf{T}(H)$ and non-negative integers m:

$$\|\,\mathrm{R}(\lambda, A)^m \rho\|_\infty \leq M'(\lambda - \beta')^{-m}\|\rho\|_\infty. \tag{138}$$

In this case, we have the explicit bound

$$\|T_t\|_\infty \leq M' e^{t\beta'} \quad \forall t > 0. \tag{139}$$

Remark B.5. It suffices that the property (137) hold for density states ρ.

Proof. To avoid duplication, we refer only to the assertions for complete positivity. By the general Hille-Yosida theory, if A is an infinitesimal generator of a contractive semigroup on $\mathbf{T}(H)$, the resolvents

$$\mathrm{R}(\lambda, A) = (\lambda - A)^{-1} \tag{140}$$

are defined for all $\lambda > 0$ and by Theorem 3.1.3 of [**30**],

$$\mathrm{R}(\lambda, A) = \int_0^\infty e^{-\lambda t} T_t dt. \tag{141}$$

i.e., the resolvent is the Laplace transform of $\{T_t\}_{t\geq 0}$. In particular, if T_t consist of completely positive operators, then the resolvent operators are all completely positive.

Conversely, let

$$A_\lambda = \lambda(\lambda\,\mathrm{R}(\lambda, A) - I) \tag{142}$$

Then for each $t \geq 0$,

$$\exp(tA_\lambda) = e^{-\lambda t}\exp\left(t\lambda^2\,\mathrm{R}(\lambda, A)\right) \tag{143}$$

which is clearly completely positive and it is known that for each $t \geq 0$,

$$T_t = \lim_{\lambda \to \infty} \exp(tA_\lambda) \tag{144}$$

in the strong operator topology. Thus T_t is completely positive.

To deal with the trace preservation properties of T_t, note that if S is a bounded operator on $\mathbf{T}(H)$ for which

$$\operatorname{tr}(S\rho) = \alpha \operatorname{tr}(\rho) \tag{145}$$

then

$$\operatorname{tr}(e^S \rho) = \sum_{k=0}^{\infty} \operatorname{tr}\left(\frac{S^k}{k!}\rho\right) = \sum_{k=0}^{\infty} \frac{\alpha^k}{k!} \operatorname{tr}(\rho) = e^{\alpha} \operatorname{tr}(\rho). \tag{146}$$

Thus,

$$\operatorname{tr}(\exp tA_\lambda \rho) = e^{-\lambda t} e^{t\lambda^2 \; 1/\lambda} \operatorname{tr}(\rho) = \operatorname{tr}(\rho). \tag{147}$$

By (144), it follows that T_t is also trace preserving. Conversely, if T_t is trace preserving,

$$\operatorname{tr}(\mathrm{R}(\lambda, A)\rho) = \int_0^\infty e^{-\lambda t} \operatorname{tr}(T_t \rho) dt = \int_0^\infty e^{-\lambda t} \operatorname{tr}(\rho) dt = \lambda^{-1} \operatorname{tr}(\rho). \tag{148}$$

□

B.1.1. *Examples of Completely Positive Semigroups.* Our analysis of the generalized Lindblad equation will reduce to an analysis of the solution in two important cases:

(Case 1) Unitary Evolution. In particular, if $\mathcal{H}$ is a self-adjoint operator on a Hilbert space H, then the family of completely positive mappings

$$P_t^{\mathcal{H}}(\rho) = e^{it\mathcal{H}} \rho e^{-it\mathcal{H}} \tag{149}$$

is a one-parameter group of completely positive maps. Its generator on the trace-class operators is formally given by the operator

$$\rho \mapsto i[\mathcal{H}, \rho]. \tag{150}$$

This expression is only formal, because it is not defined for all ρ. Nevertheless, the infinitesimal generator is densely defined on the space of trace-class operators and it is an extension of (150) for the finite rank operators on the domain of $\mathcal{H}$.

(Case 2) Dissipative Operators. Another type of infinitesimal generator we will consider are operators of the form

$$\mathcal{L}\rho = \sum_j \left[L_j \rho L_j^\dagger - \frac{1}{2} \{ L_j^\dagger L_j, \rho \} \right] \tag{151}$$

where braces denote the anti-commutator.

Lemma B.6. *Suppose*

$$\sum_j L_j^\dagger L_j \in \mathbf{L}(H). \tag{152}$$

Then the operator given by (151) *is bounded on* $\mathbf{T}(H)$. *If in addition*

$$\sum_j L_j L_j^\dagger \in \mathbf{L}(H). \tag{153}$$

then $\mathcal{L}$ *is a bounded operator on* $\mathbf{L}(H)$.

Proof. Let C be the operator norm of $\sum_j L_j^\dagger L_j$. To show the map $\mathcal{L}$ is defined and continuous on $\mathbf{T}(H)$, it suffices to show $\mathcal{L}_0 : \rho \mapsto \sum_j L_j \rho L_j^\dagger$ is defined and continuous on $\mathbf{T}(H)$. However, if $\rho \geq 0$,

$$\operatorname{tr}(\mathcal{L}_0(\rho)) = \sum_i \operatorname{tr}(L_j \rho L_j^\dagger) \tag{154}$$

$$= \sum_j \operatorname{tr}(\rho L_j^\dagger L_j) \tag{155}$$

$$= \sum_j \operatorname{tr}\Big(\rho^{1/2} L_j^\dagger L_j \rho^{1/2}\Big) \tag{156}$$

$$= \operatorname{tr}\Big(\rho^{1/2} (\sum_j L_j^\dagger L_j) \rho^{1/2}\Big) \leq C \operatorname{tr}(\rho) = C\|\rho\|_1 \tag{157}$$

thus for arbitrary self-adjoint ρ,

$$\|\mathcal{L}_0(\rho)\|_1 = \|\mathcal{L}_0(\rho^+ - \rho^-)\|_1 \tag{158}$$

$$\leq \|\mathcal{L}_0(\rho^+)\|_1 + \|\mathcal{L}_0(\rho^-)\|_1 \tag{159}$$

$$\leq C\Big(\|\rho^+\|_1 + \|\rho^-\|_1\Big) = C\|\rho\|_1. \tag{160}$$

If (153), suppose $0 \leq T \leq 1$:

$$0 \leq \sum_j L_j^\dagger T L_j \leq \sum_j L_j^\dagger L_j \leq C 1_H \tag{161}$$

Thus, for arbitrary T,

$$\|\mathcal{L}T\|_\infty \leq \|\sum_j L_j L_j^\dagger\|_\infty + C\|T\|_\infty \tag{162}$$

□

It was established by Lindblad [**21**] (and not too hard to show directly) that if (152) holds, the $\mathcal{L}$ generates a *uniformly continuous* a completely positive semigroup (relative to the operator norm on $\mathbf{T}(H)$). In this case the semigroup is given by

$$e^{t\mathcal{L}} = \sum_{k=0}^\infty \frac{t^k}{k!} \mathcal{L}^k\ . \tag{163}$$

B.2. Perturbation of Completely Positive Generators. In order to show that the generalized Lindblad operators given in equation (60) are completely positive generators, we need to establish a perturbation result analogous to the Kato-Rellich theorem.

A linear map B on $\mathbf{T}(H)$ is *trace annihilating* iff

$$\operatorname{tr}(B\rho) = 0 \tag{164}$$

for all $\rho \in \mathbf{T}(H)$. For example, an operator of the form (151) is easily seen to be trace annihilating.

Using the Trotter-Kato product formula ([**31**], [**5**]), we can show that generators of completely positive contractive semigroups have a sum which is also a generator of a contractive semigroup, provided the sum generates a contractive semigroup.

PROPOSITION B.7. *Suppose B is a bounded operator of the form* (151). *If A is a generator of a completely positive semigroup then so is $A + B$. .*

COROLLARY B.8. *The generalized Lindblad operators given in equation* (60) *generate a completelty positive semigroup of contractions on $\mathbf{T}(H)$.*

We now extend the results of Lindblad and Davies to allow for time varying Hamiltonians by relying on results of Kato. The need for this arises since in some circuit-based models the various gates are implemented by varying the Hamiltonian (see for instance [**23**] §7.7.2). We make the assumption that the dissipative effects are bounded which simplifies the analysis considerably.

B.3. Solving the Generalized Lindblad Equation. In some cases it is possible to solve the generalized Lindblad equation [**22**]. However, by solution we mean an expression for the fundamental solution $P_{t,s}$ as a limit of product of exponentials. Though this expression will almost never provide a closed form solution, it will provide enough information to obtain an estimate of how well a unitary (or partial isometry) can be implemented by one of the operators $P_{t,s}$. The two tools we use are the Trotter-Kato product formula and the explicit form of the solution of a time-dependent equation as a time ordered product of exponentials given in the proof of §4.2 of [**30**].

A precise formulation of a set of conditions which guarantees the convergence of the products in the next two theorems is given in Theorem B.11. These results comprised by Theorems B.9 and B.10 are restatements of assertions contained in the proofs in §4.2 of [**30**].

THEOREM B.9. *Under suitable conditions, the fundamental solution $P_{t,s}$ for* (62) *is given by*

$$P_{t,s} = \text{str-lim}_{\Delta \to 0} \prod_{k=0}^{n-1} \exp\bigl((r_{k+1} - r_k) A(r_k)\bigr), \tag{165}$$

where $s = r_0 < r_1 < \cdots < r_{n-1} < t$ and $\max |r_{k+1} - r_k| \leq \Delta$. Each $P_{t,s}$ is completely positive and trace preserving.

THEOREM B.10. *Under the same assumptions as the previous theorem B.9,*

$$\exp sA(t) = \text{str-lim}_{n \to \infty} \exp\left(\frac{s}{n}\mathcal{L}(t)\right) \, \exp\left(\frac{s}{n}\mathcal{H}(t)\right) \tag{166}$$

B.4. Existence of Solutions. We will restrict our attention to bounded time varying perturbations of a fixed self-adjoint operator acting on $\mathbf{T}(H)$ via a commutator as in (167) below. The result we state is not the most general possible, and the early results of Kato [**14**] suffice for its proof. We follow the treatment in Chapter XIV, §4 of [**34**] which is a more readily available reference.

THEOREM B.11. *Suppose $\mathcal{H}$ is a self-adjoint operator, $\{B(t)\}_{t \in [0,\infty[}$, $\{L_j(t)\}_{t \in [0,\infty[}$, $1 \leq j \leq n$ are families of bounded operators, all of which are continuously norm* *differentiable as a functions of t, then there is a fundamental solution $P_{t,s}$ for* (62) *where*

$$A(t)\rho = -i[\mathcal{H} + B(t), \rho] + \sum_{j=1}^{n} \left(L_j(t)\rho L_j^\dagger(t) - \frac{1}{2}\big\{L_j^\dagger(t) L_j(t), \rho\big\} \right). \tag{167}$$

The solution is a given by a limit of a time-ordered product of exponentials (165).

Proof. There are various technical assumptions for a family $A(t)$ of operators that need to be checked in order to apply Kato's Theorem. The first of these is the independence of $\operatorname{dom} A(t)$ of the parameter t. Under our assumptions

$$A(t) = A + C(t) \tag{168}$$

where $C(t) : \mathbf{T}(H) \to \mathbf{T}(H)$ are bounded operators and A is the infinitesinal generator of a contractive semigroup. Indeed,

$$A\rho = -i[\mathcal{H}, \rho] \tag{169}$$

is the infinitesimal generator of a group on $\mathbf{T}(H)$ and

$$C(t)\rho = -i[B(t), \rho] + \sum_{j=1}^{n} \left(L_j(t)\rho L_j^\dagger(t) - \frac{1}{2}\big\{L_j^\dagger(t) L_j(t), \rho\big\} \right). \tag{170}$$

is by assumption a bounded operator on $\mathbf{T}(H)$. In particular, all the operators $A(t)$ have the same domain $\operatorname{dom}(A)$.

We now address the remaining assumptions in Kato's theorem. For any $\lambda > 0$,

$$\lambda - A(t) = \lambda - A - C(t) = (I + C(t)\,\mathrm{R}(\lambda, A))(\lambda - A) \tag{171}$$

For λ sufficiently large $\mathrm{R}(\lambda, A)C(t)$ has norm < 1, so the Neumann (geometric) series for inverses (see [**9**], Chapter VIII, §3) $I + \mathrm{R}(\lambda, A)C(t)$ is invertible. Thus we can write,

$$(\lambda - A(t))^{-1} = \mathrm{R}(\lambda, A)(I + \mathrm{R}(\lambda, A)C(t))^{-1} \tag{172}$$

Thus,

$$B(t, s) = (\lambda - A(t))(\lambda - A(s))^{-1} = (I + C(t)\,\mathrm{R}(\lambda, A))(I + C(s)\,\mathrm{R}(\lambda, A))^{-1} \tag{173}$$

is well defined and by our assumptions $B(t, s)$ is a norm differentiable function jointly in the variables t, s. This implies the remaining conditions in the hypothesis of Kato's theorem. It only remains to observe that presence of the parameter λ, instead of 1 as actually stated in Kato's theorem is immaterial, since solutions of equations

$$\frac{d}{dt}\rho(t) = A(t)\rho(t) \tag{174}$$

are trivially affected by adding a constant scalar to $A(t)$. □

Appendix C. Solving the Ersatz Quantum Computer Condition

Consider the ersatz quantum computer condition ($\mathcal{E}$QCC) given in (3):

$$P \cdot \rho = U \rho U^\dagger. \tag{175}$$

Note that this can be obtained by setting the encoding and decoding maps to unity, and setting $\alpha = 0$ in the QCC given in (12). A simple observation shows that "solving" (175) is completely equivalent to obtaining the noise-free part of a communication channel.

Theorem C.1. *Suppose H is finite-dimensional. If P is given by the Kraus representation* (127)*, given a unitary U, the set of $\rho \in \mathbf{L}(H)$ satisfying* (175) *is the $*$-subalgebra of $\mathbf{L}(H)$ given by*

$$\mathfrak{A}_{P,U} = \{\rho \in \mathbf{L}(H) : \forall i \in I, \quad [\rho, U^\dagger X_i] = 0\} \tag{176}$$

Proof. The solutions of (175) are the fixed points of the completely positive map Q defined by the equation

$$Q \cdot \rho = \sum_{i \in I} U^\dagger X_i \rho X_i^\dagger U. \tag{177}$$

Now apply [**17**], Theorem 2.1. □

In the above theorem, the assumption H is finite-dimensional is essential, see [**3**]. Since H is finite dimensional $\mathfrak{A}$ is an algebraic direct sum of algebras isomorphic to full matrix algebras.

Proposition C.2. *Let $\{E_\kappa\}_{\kappa \in I}$ be the set of finite-dimensional minimal central projections of $\mathfrak{A}$. Then*

$$\mathfrak{A}_\kappa = E_\kappa \mathfrak{A} E_\kappa \tag{178}$$

is an algebra of operators on the range H_κ of E_κ (which is a finite dimensional space). It is isomorphic to a full matrix-algebra of finite multiplicity.

References

[1] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," *Proc. 29th Ann. ACM Symp. on Theory of Computing*, p. 176 (New York, ACM, 1998), arXiv:quant-ph/9611025.

[2] P. Aliferis, D. Gottesman, J. Preskill, "Quantum Accuracy Threshold for Concatenated Distance-3 Codes," arXiv:quant-ph/0504218 (2005).

[3] A. Arias, A. Gheondea, and S. Gudder. Fixed points of quantum operations. *J. Mathematical Physics*, 43(12):5872–5881, 2002.

[4] S.C. Benjamin, J. Eisert, and andT.M. Stace4. Optical generation of matter qubit graph states. *arXiv:quant-ph/0506110.*

[5] P. R. Chernoff. Note on product formulas for operator semigroups. *Journal of Functional Analysis*, 2:238–243, 1968.

[6] M. D. Choi. Positive Linear Maps on C*-algebras. *Can. J. Math*, XXIV (3): 520-529, 1972.

[7] A. Connes. *Noncommutative Geometry.* Academic Press, 1994.

[8] D. Deutsch. Quantum computational networks. *Proc. Roy. Soc. London*, A425:73–90, 1989.

[9] J. Dieudonné *Foundations of Modern Analysis.* Academic Press, 1960.

[10] J. Dixmier. *Les algèbres d'opérateurs dans l'espace hilbertien.* Gauthier Villars, Paris, 1969.

[11] M. H. Freedman, A. Kitaev, M. J. Larsen, and Z. Wang. Topological quantum computation. *Bulletin of the American Mathematical Society*, 40(1):216, 2003.

[12] I. C. Gohberg and M. G. Krein. *Introduction to the theory of linear nonselfadjoint operators.* American Mathematical Society, Providence, R. I., 1969.

[13] D. Gottesman, “Stabilizer codes and quantum error correction,” Caltech Ph.D. thesis, 1997, arXiv:quant-ph/9705052.

[14] T. Kato. Integration of the equation of evolution in a Banach space. *J. Math. Soc. of Japan*, 5:208–234, 1953.

[15] A. Kitaev. Quantum computations: Algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[16] E. Knill, R. Laflamme, W. H. Zurek, “Resilient quantum computation: error models and thresholds,” Proc. Roy. Soc. London A **454**, 365 (1998), arXiv:quant-ph/9702058.

[17] D. W. Kribs. Quantum channels, wavelets, dilations and representations of O_n. *arXiv:math.OA/0309390*.

[18] D. Kribs, R. Laflamme, D. Poulin, “A Unified and Generalized Approach to Quantum Error Correction,” *Phys. Rev. Lett.* 94: 180501, 2005, arXiv:quant-ph/0412076.

[19] D. Kribs, R. Laflamme, D. Poulin, M. Lesosky “Operator Quantum Error Correction,” arXiv:quant-ph/0504189 (2005).

[20] D. A. Lidar, D. Bacon, K. B. Whaley, “Concatenating Decoherence Free Subspaces with Quantum Error Correcting Codes,” *Phys. Rev. Lett.*, 82:4556, 1999, arXiv:quant-ph/9809081.

[21] G. Lindblad. On the generators of quantum dynamical semigroups. *Communications in Mathematical Physics*, 48(119), 1976.

[22] H. X. Lu, J. Yang, Y.D. Zang, and Z. B. Chen. Algebraic approach to master equations with superoperator generators of su(1,1) and su(2) lie algebras. *Phys. Rev. A*, 67(12), 2003.

[23] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[24] J. Preskill, “Reliable quantum computers,” Proc. Roy. Soc. Lond. A **454**, 385-410 (1998), arXiv:quant-ph/9705031.

[25] R. Raussendorf and H. J. Briegel. Computational model for the one-way quantum computer: Concepts and summary. *arXiv:quant-ph/0207183*.

[26] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[27] R. Raussendorf, D.E. Browne, and H.J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A*, 68: 022312, 2003.

[28] P.W. Shor, “Fault-tolerant quantum computation,” in *Proceedings, 37th Annual Symposium on Foundations of Computer Science*, pp. 56-65 (Los Alamitos, CA, IEEE Press, 1996), arXiv:quant-ph/9605011.

[29] W. F. Stinespring. Positive Functions on C*-algebras. *Proc. Amer. Math. Soc.*, 6: 211-216, 1955.

[30] H. Tanabe. *Equations of Evolution*. Pitman, London,, 1975.

[31] H. F. Trotter. On the products of semi-groups of operators. *Proc. Amer. Math. Soc.*, 10:554–551, 1959.

[32] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, New Jersey, 1955.

[33] Y.S. Weinstein, T. Havel, J. Emerson, N. Boulant, M. Saraceno, S. Lloyd, D. Cory. “Quantum Process Tomography of the Quantum Fourier Transform,” *J. Chem. Phys*, **121**, 6117, 2004.

[34] K. Yosida *Functional Analysis*. Springer-Verlag, New York, 1968.

[35] C. Zalka, Threshold estimate for fault tolerant quantum computing, arXiv:quant-ph/9612028, 1996.